Dodatek č. 1
ke Smlouvě o poskytování služeb ISMS

Objednatel:	Dopravní společnost Ústeckého kraje, příspěvková organizace
se sídlem:	Velká Hradební 3118/48; 400 01 Ústí nad Labem
zastoupený:	Ing. Milan Šlejtr, ředitel
IČO:	06231292
DIČ:	CZ06231292
bankovní spojení:	[redacted]
č. účtu:	[redacted]

zapsaný v OR vedeném Krajským soudem v Ústí nad Labem, spis. zn. Pr, vložka 1129

(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:	u Městského soudu v Praze, sp. zn. C 279627

(dále jen „**Poskytovatel**")

(Objednatel a Poskytovatel společné též jako „**Smluvní strany**")

uzavírají tento dodatek č. 1 ke Smlouvě o poskytování služeb
(dále **jen „Dodatek"**)

I.
Úvodní ustanovení

1. Smluvní strany konstatují, že dne 30.12.2024 uzavřely Smlouvu o poskytování služeb ISMS, jejímž předmětem byl především závazek Poskytovatele poskytnout Objednateli předem sjednané služby specifikované ve smlouvě (dále jen „**Smlouva**").
2. Smluvní strany se tímto Dodatkem rozhodly upravit rozsah a definici Služeb popsaných ve Smlouvě, jakož i cenu za jejich poskytnutí.
3. Služby se týkají kybernetické bezpečnosti a ISMS. V tomto smyslu tak smluvní strany upravují plnění smlouvy a její přílohu tímto dodatkem.
4. Příloha Smlouvy uvádí, že předmětem Smlouvy jsou Služby směřující k zajištění kybernetické bezpečnosti v režimu nižších povinností. Při poskytování Služeb dle Smlouvy však bylo zjištěno, že Objednatel spadá do režimu vyšších povinností, a to v důsledku zavedení jednotek pro preferenci vozidel (organizace poskytuje regulovanou službu, dle bodu 15.2 Provoz inteligentního dopravního systému). V důsledku toho vzniká potřeba poskytnout některé další služby, nad rámec těch uvedených ve Smlouvě před uzavřením tohoto Dodatku. S tím souvisí

i navýšení ceny za poskytnutí Služeb. V tomto smyslu Smluvní strany upravují Smlouvu tímto Dodatkem, jak je uvedeno následovně.

II.
Změnová ujednání

1. Smluvní strany tímto Dodatkem upravují znění článku 2: ÚVODNÍ USTANOVENÍ, když nově zní tento článek 2. takto:

   „2. ÚVODNÍ USTANOVENÍ

   2.1. Účelem této smlouvy je zavedení požadavků kybernetické bezpečnosti na Poskytovatele regulované služby v režimu vyšších povinností u Objednatele, 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 (směrnice NIS 2) a zákona č. 264/2025, o kybernetické bezpečnosti, v platném znění (dále jen „ZKB") a navazujících vyhlášek.

   *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 vyhlášky č.409/2005 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále také „**Vyhláška**").*

   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 (zejm. Vyhlášky)."

2. Smluvní strany tímto Dodatkem mění rozsah Služeb z režimu nižších povinností do režimu vyšších povinností. Protože původní Smlouva popisovala Služby týkající se nižších povinností a stanovovala cenu za jejich poskytnutí, mění Smluvní strany tímto Dodatkem Služby tak, aby odpovídaly plnění bezpečnostních opatření Objednatele v režimu vyšších povinností. Změna *Služeb (rozdíl služeb při nižších a vyšších povinnostech)* oproti službách, jak byly popsány v příloze Smlouvy před uzavřením tohoto Dodatku, je uvedena v příloze tohoto Dodatku. Smluvní strany se tak dohodly, že Poskytovatel bude poskytovat Služby odpovídajícím službám v režimu vyšších povinností, jak je stanoveno v této příloze. Protože některé služby jsou v obou režimech shodné, příloha tohoto Dodatku nenahrazuje, pouze doplňuje přílohu Smlouvy.

3. Smluvní strany se dohodly na změně znění odst. 3.4., když nově zní odst. 3.4 takto:

   „3.4 Služby jsou Poskytovatelem poskytnuté řádně splněním 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."

4. Smluvní strany se dohodly na změně znění odst. 3.5., když nově zní odst. 3.5 takto:

   „3.5. *Služby budou poskytovány Objednateli postupně po jednotlivých etapách, a to:*
   Etapa 1: Služby k zajištění souladu zpracovávaných osobních údajů s požadavky GDPR
   Etapa 2: Implementace NIS 2
   Etapa 3: Vytvoření funkční Politiky IT bezpečnosti

5. V souvislosti se změnou rozsahu Služeb se Smluvní strany dohodly i na změně ceny. Smluvní strany se tak dohodly na změně znění odst. 4.1. a nově zní odst. 4.1 takto:

„4.1 Objednatel se zavazuje uhradit Poskytovateli za provedené Služby odměnu celkem ve výši 1 116 500,- Kč bez DPH (dále jen „Cena"). Cena se skládá z následujících dílčích odměn:

4.1.1. Etapa 1: 174 000,-Kč bez DPH

4.1.2. Etapa 2: 652 500,-Kč bez DPH

4.1.3. Etapa 3: 290 000,-Kč bez DPH"

Cenu se Objednatel zavazuje uhradit postupně, a to po jednotlivých etapách. Nárok Poskytovatele na úhradu odměny za jednotlivou etapu vzniká okamžikem poskytnutí Služeb v rámci dané etapy ve smyslu odst.3.4, 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.

6. Smluvní strany se dohodly na změně znění odst. 5.1. a nově zní odst. 5.1 takto:

   „5.1. Poskytovatel se zavazuje zahájit plnění Služeb dle této Smlouvy bez zbytečného odkladu po podpisu Smlouvy oběma Smluvními stranami, a to tak, aby Služby byly poskytnuty nejpozději do 07/2026."

7. Smluvní strany se dohodly na změně znění odst. 5.2. a nově zní odst. 5.2 takto:

   „5.2. Služby v rámci dané etapy jsou poskytnuty ve smyslu odstavce 4, 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. V případě, že není mezi Smluvními stranami dohodnut výstup z dané Služby, je Služba poskytnuta splněním poslední činnosti z dané Služby. O splnění Služby informuje Poskytovatel Objednatele. K poskytnuté Službě může Objednatel vznést připomínky nejpozději do 5 pracovních dnů od oznámení o poskytnutí Služby. Pokud v uvedené lhůtě Objednatel nesdělí své připomínky, považují se poskytnuté Služby za řádně poskytnuté a Objednatel je povinen podepsat akceptační protokol bez výhrad. Jsou-li k poskytnutým Službám vzneseny oprávněné připomínky, zapracuje je Poskytovatel v přiměřené lhůtě. Poskytnutím Služby zohledňující připomínky dle předchozí věty vzniká Objednateli povinnost k podpisu akceptačního protokolu."

8. Všechna ostatní ujednání Smlouvy zůstávají beze změn.

III.
Závěrečná ustanovení

1. Tento Dodatek se řídí českým právním řádem, zejména občanským zákoníkem.
2. V případě, že se některé ustanovení tohoto Dodatku 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.
3. Tento Dodatek nabývá účinnosti 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), ve znění pozdějších předpisů, kdy jeho zveřejnění zajistí Objednatel.

4. Tento Dodatek je vyhotoven ve dvou (2) stejnopisech, z nichž Objednatel obdrží jeden (1) a Poskytovatel jeden (1) stejnopis.
5. Smluvní strany shodně prohlašují, že si Dodatek před jeho podpisem přečetli, že byl uzavřen po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni za nápadně nevýhodných podmínek. Smluvní strany potvrzují autentičnost Dodatku svým podpisem.
6. Přílohou tohoto dodatku je prezentace popisující rozdíl ve službách v režimu nižších a vyšších povinnostech.

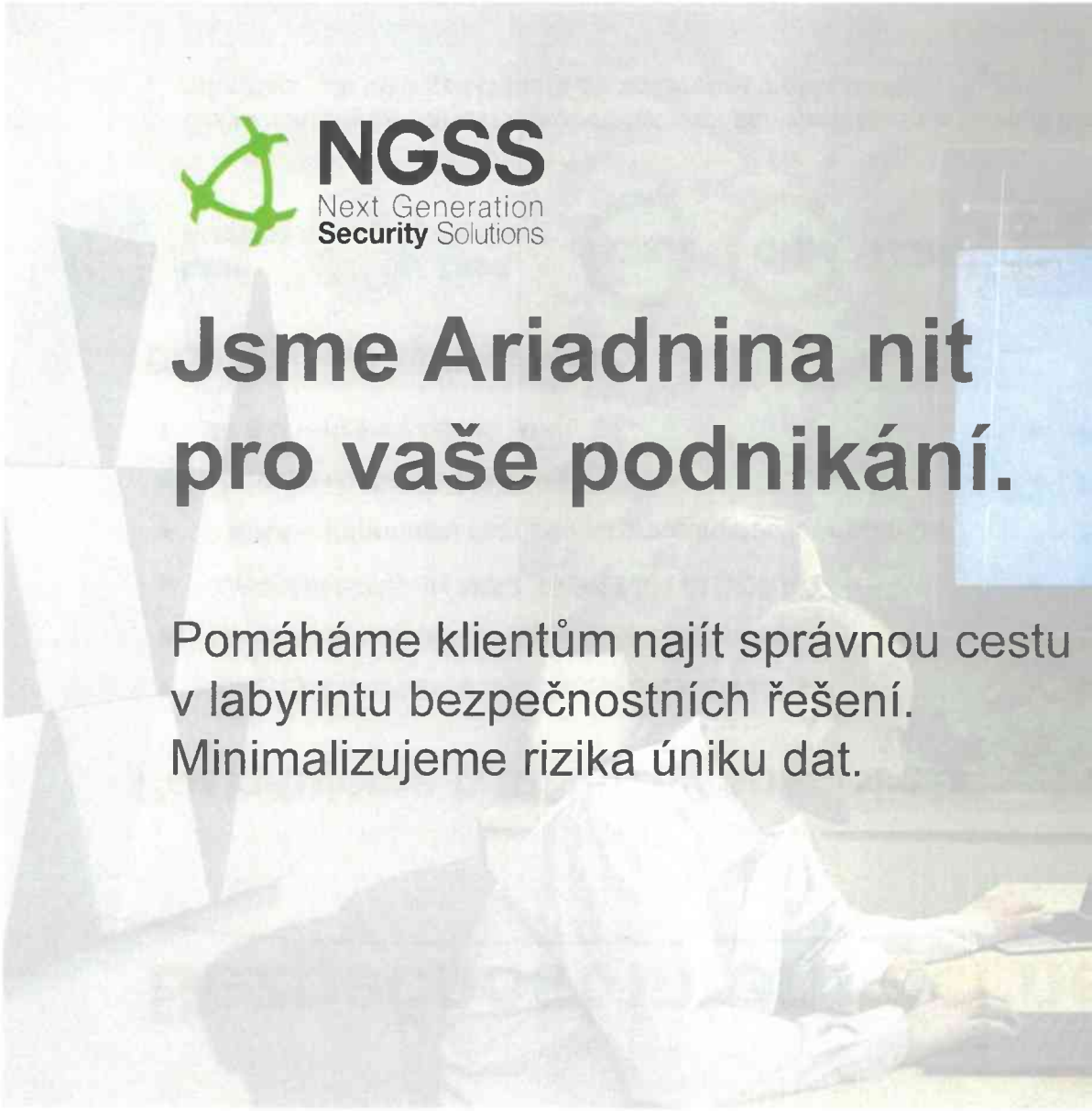
V Ústí nad Labem, dne .....

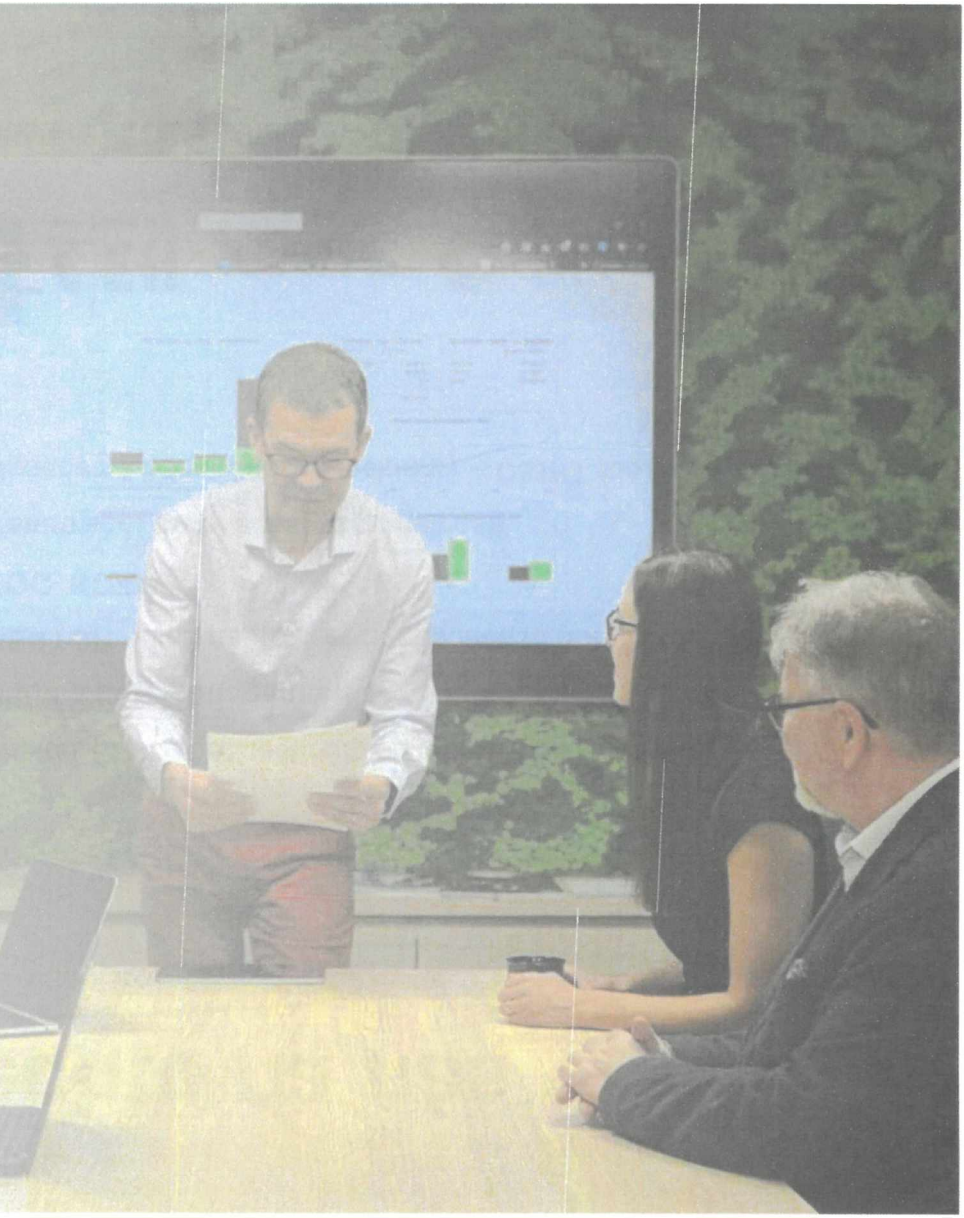
V Praze dne .....

[redacted]

Dopravní společnost Ústeckého kraje, příspěvková organizace
Ing. Milan Šlejtr, ředitel

Next Generation Security Solutions s.r.o.
Mgr. Ondřej Dedek, jednatel


NGSS
Next Generation
Security Solutions
Jsme Ariadnina nit
pro vaše podnikání.
Pomáháme klientům najít správnou cestu
v labyrintu bezpečnostních řešení.
Minimalizujeme rizika úniku dat.



Bezpečnost informací nechte na nás

Poskytujeme tyto služby specialistů:

- Analýzy a hodnocení rizik, bezpečnostní **audity**
- Konzultace a školení kybernetické bezpečnosti
- Zavádění ISMS dle **NIS2**, **ISO 27001 či DORA**
- **TISAX** – Informační bezpečnost pro automobilový průmysl
- Ochrana osobních údajů, **GDPR**
- **AI Act** – rizika v oblasti AI
- Implementace bezpečnostních technologií a projektů
- SIEM a **Log Management**
- **NESTOR** – váš nepřetržitý bezpečnostní dohled - SIEM, SOC, SOAR
- **Penetrační testy** a testy zranitelností
- Reakce na bezpečnostní incidenty – **CSIRT team**

Disponujeme certifikacemi:

ISO 27001 Lead Auditor · ISO 20000 Lead Auditor · CISM · CISA · CRISC · CISSP · CEH Certified Ethical Hacker · TOGAF · ITIL · PRINCE2 · CCSP · CERTIFIED BY TI TRUSTED INTRODUCER

Díky spolupráci s partnery, mohou být součástí týmu nejen odborníci zaměření na bezpečnost informací, ale také **specialisté se znalostmi v oblasti ICT**.

Naše zkušenosti

VoZP | VOJENSKÁ ZDRAVOTNÍ POJIŠŤOVNA

AUDITOR Audit • Tax • Accounting

PRIMAPOL

global assistance

PRAHA PRAGUE PRAGA PRAG

MĚSTSKÁ ČÁST PRAHA 2

voestalpine

ČZU Česká zemědělská univerzita v Praze

MĚSTSKÁ ČÁST PRAHA 9

arriva

euroawk THE GREAT OUTDOORS.

DATRON INFORMATION TECHNOLOGIES

SIEMENS

Sellier & Bellot

STROJMETAL aluminium forging


globus


CPI
Property
Group


Dopravní podnik
hlavního města Prahy


FNO
FAKULTNÍ
NEMOCNICE
OSTRAVA


MĚSTSKÁ POLICIE
PRAHA


penta
HOSPITALS.CZ


UNIVERZITA
KARLOVA


ŠKODA


randstad


BIOLOGICKÉ
CENTRUM
AV ČR, v. v. i.


VFN
PRAHA


FutureLife


Orkla
Food Ingredients
Česko


FAKULTNI
NEMOCNICE
U SV. ANNY
V BRNE


NGSS
Next Generation
Security Solutions

Rozdíl vyšších a nižších povinností

Vyhláška č. 410/2025 Sb. – nižší režim

- § 1 – Předmět úpravy
- § 2 – Vymezení pojmů
- § 3 – Systém zajišťování minimální kybernetické bezpečnosti
- § 4 – Požadavky na vrcholné vedení
- § 5 – Bezpečnost lidských zdrojů
- § 6 – Řízení kontinuity činností
- § 7 – Řízení přístupu
- § 8 – Řízení identit a jejich oprávnění
- § 9 – Detekce a zaznamenávání KBU
- § 10 – Řešení KBI
- § 11 – Bezpečnost komunikačních sítí
- § 12 – Aplikační bezpečnost
- § 13 – Kryptografické algoritmy
- § 14 – Stanovení významnosti dopadu KBI

Vyhláška č. 409/2025 Sb. – vyšší režim

- § 1 – Předmět úpravy
- § 2 – Vymezení pojmů
- § 3 – Systém řízení bezpečnosti informací
- § 4 – Požadavky na vrcholné vedení
- § 5 – Stanovení bezpečnostních rolí
- § 6 – Řízení bezpečnostní politiky a bezpečnostní dokumentace
- § 7 – Řízení aktiv
- § 8 – Řízení rizik
- § 9 – Řízení dodavatelů
- § 10 – Bezpečnost lidských zdrojů
- § 11 – Řízení změn
- § 12 – Akvizice, vývoj a údržba
- § 13 – Řízení přístupu
- § 14 – Zvládání kybernetických bezpečnostních událostí a incidentů
- § 15 – Řízení kontinuity činností
- § 16 – Provádění auditu kybernetické bezpečnosti
- § 17 – Fyzická bezpečnost

NGSS
Next Generation Security Solutions

Rozdíl vyšších a nižších povinností

Vyhláška č. 409/2025 Sb. – vyšší režim

- § 18 – Bezpečnost komunikačních sítí
- § 19 – Správa a ověřování identit
- § 20 – Řízení přístupových práv a oprávnění
- § 21 – Detekce kybernetických bezpečnostních událostí
- § 22 – Zaznamenávání událostí
- § 23 – Vyhodnocování KBI
- § 24 – Aplikační bezpečnost
- § 25 – Kryptografické algoritmy
- § 26 – Zajištění dostupnosti regulované služby
- § 27 – Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

NGSS
Next Generation
Security Solutions

Bezpečnostní politiky

Vyhláška č. 410/2025 Sb. – nižší režim

1. Politika zajišťování minimální úrovně kybernetické bezpečnosti
2. Politika bezpečnosti lidských zdrojů
3. Politika řízení kontinuity činností
4. Politika řízení přístupu
5. Politika detekce kybernetických bezpečnostních událostí a řešení kybernetických bezpečnostních incidentů
6. Politika bezpečnosti komunikační sítě
7. Politika aplikační bezpečnosti

Vyhláška č. 409/2025 Sb. – vyšší režim

1. Politika systému řízení bezpečnosti informací
2. Politika organizační bezpečnosti
3. Politika řízení bezpečnostní politiky a dokumentace
4. Politika řízení aktiv
5. Politika řízení rizik
6. Politika řízení dodavatelů
7. Politika bezpečnosti lidských zdrojů
8. Politika bezpečného chování uživatelů, administrátorů a osob zastávajících bezpečnostní role
9. Politika bezpečného používání mobilních zařízení
10. Politika řízení změn

NGSS
Next Generation
Security Solutions

Bezpečnostní politiky

Vyhláška č. 409/2025 Sb. – vyšší režim

11. Politika akvizice, vývoje a údržby
12. Politika řízení přístupu
13. Politika zvládání kybernetických bezpečnostních událostí a incidentů
14. Politika řízení kontinuity činností
15. Politika fyzické bezpečnosti
16. Politika bezpečnosti komunikační sítě
17. Politika pro zaznamenávání událostí
18. Politika nasazení, používání a údržby nástrojů pro detekci kybernetických bezpečnostních událostí a nástroje pro sběr a vyhodnocování kybernetických bezpečnostních událostí
19. Politika řízení zranitelností a patch management
20. Politika používání kryptografie
21. Politika dlouhodobého ukládání, zálohování a obnovy

NGSS
Next Generation
Security Solutions

Obsah bezpečnostní dokumentace

Vyhláška č. 410/2025 Sb. – nižší režim

1. Evidence aktiv
2. Přehled bezpečnostních opatření
3. Plány obnovy
4. Závěrečná zpráva o kybernetickém bezpečnostním incidentu
5. Evidence nepodporovaných technických aktiv

Vyhláška č. 409/2025 Sb. – vyšší režim

1. Plán provádění auditu kybernetické bezpečnosti
2. Zpráva z auditu kybernetické bezpečnosti
3. Zpráva z přezkoumání systému řízení bezpečnosti informací
4. Metodika pro identifikaci a hodnocení aktiv
5. Metodika pro identifikaci a hodnocení rizik
6. Zpráva o hodnocení aktiv a rizik
7. Prohlášení o aplikovatelnosti
8. Plán zvládání rizik

NGSS
Next Generation
Security Solutions

Obsah bezpečnostní dokumentace

Vyhláška č. 409/2025 Sb. – vyšší režim

9. Plán rozvoje bezpečnostního povědomí
10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků
11. Metodika pro provedení analýzy dopadů
12. Plány kontinuity činností
13. Plány obnovy
14. Evidence technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována
15. Evidence technických aktiv, účtů a autentizačních mechanismů, které nesplňují požadavek na vícefaktorovou autentizaci

NGSS
Next Generation
Security Solutions

Další doporučená dokumentace

Vyhláška č. 410/2025 Sb. – nižší režim

1. Topologie infrastruktury
2. Segmentace infrastruktury
3. Přehled technických aktiv zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů
4. Kontakty na osoby pověřené technickou a systémovou podporou

Vyhláška č. 409/2025 Sb. – vyšší režim

1. Topologie infrastruktury
2. Segmentace infrastruktury
3. Přehled technických aktiv v rozsahu systému řízení bezpečnosti informací, zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů
4. Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory

NGSS
Next Generation
Security Solutions

NGSS
Next Generation
Security Solutions

Děkujeme za váš čas a vaši pozornost

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

NGSS
Next Generation
Security Solutions