Zmluva o zabezpečení plnenia bezpečnostných opatrení
a notifikačných povinností
uzatvorená v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
(ďalej len „Zmluva“)

medzi zmluvnými stranami:

| | |
|---|---|
| Prevádzkovateľ: | **Obec Bernolákovo** |
| Sídlo: | Hlavná 111, Bernolákovo 900 27 |
| IČO: | 00 304 662 |
| DIČ: | 2020662028 |
| Zastúpený: | Ing. Miroslav Turenič, MBA, LL.M., starosta obce |

(ďalej len „Prevádzkovateľ základnej služby" alebo „obec“)

a

| | |
|---|---|
| Dodávateľ: | **ESKAVER s. r. o.** |
| Sídlo: | Hviezdoslavova 1, Senec 903 01 |
| IČO: | 52 739 449 |
| IČ DPH: | SK2121165904 |
| Zastúpený: | Andrea Belanová, konateľ |
| Zapísaný: | Obchodný register Mestského súdu Bratislava III., oddiel Sro, vložka č. 142573/B |

(ďalej len „Dodávateľ")

(Prevádzkovateľ základnej služby a Dodávateľ spolu ďalej len „zmluvné strany“)

## Článok I.
## ÚVODNÉ USTANOVENIA

1. Organizácia je Prevádzkovateľom základnej služby podľa ustanovenia § 3 písmena k, l zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „zákon o kybernetickej bezpečnosti“) a je povinný plniť povinnosti v zmysle vyhlášky č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len vyhláška č. 362/2018 Z. z.“).
2. Identifikovanou základnou službou Prevádzkovateľa základnej služby je:
   Správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

Sektor: Verejná správa
Podsektor: Informačné systémy verejnej správy

3. Prevádzkovateľom základnej služby a Dodávateľ uzavreli dňa 15.01.2024 Zmluvu o vykonávaní správy serverov, počítačovej a metropolitnej siete a kamerového systému (ďalej len „zmluva o poskytovaní služieb“), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v zákone o kybernetickej bezpečnosti pre Prevádzkovateľa základnej služby.
4. V súlade s ustanovením § 19 ods. 2 zákona o kybernetickej bezpečnosti je Prevádzkovateľ základnej služby povinný pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa základnej služby (ďalej len „tretia strana“) uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona o kybernetickej bezpečnosti počas celej doby platnosti zmluva o poskytovaní služieb.
5. Zmluva stanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Prevádzkovateľa základnej služby a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany Prevádzkovateľa základnej služby (ďalej len „ciele"), a to aj v spolupráci s Dodávateľom.
6. Plnenie povinností podľa tejto Zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania zmluvy.

## Článok II.
## DEFINÍCIA ZÁKLADNÝCH POJMOV

Na účely tejto Zmluvy znamená pojem:

a) bezpečnostný incident - nežiaduca udalosť, pri ktorej existuje vysoká pravdepodobnosť ohrozenia bezpečnosti (dostupnosti, dôvernosti a integrity) informácií obce,
b) digitálna služba – služba, ktorej druh je uvedený prílohe č. 2 k zákonu o kybernetickej bezpečnosti,
c) dostupnosť – záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
d) dôvernosť – záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
e) hrozba – každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
f) Informačný systém – funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov.
g) integrita – záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
h) JISKB - Jednotný informačný systém kybernetickej bezpečnosti v správe Národného bezpečnostného úradu (ďalej len „NBÚ“); slúži ako systém včasného varovania a zároveň ako systém na nahlasovanie kybernetických bezpečnostných incidentov podľa Vyhlášky č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
i) kontinuita – strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
j) kybernetická bezpečnosť – stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť

uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

k) kybernetický bezpečnostný incident – akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť, alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií,

l) kybernetický priestor – globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

m) manažér kybernetickej bezpečnosti – zodpovedá za riadenie a koordináciu kybernetickej a informačnej bezpečnosti, určovanie zásad, tvorbu a aktualizáciu Bezpečnostnej stratégie kybernetickej bezpečnosti a Bezpečnostnej politiky kybernetickej bezpečnosti a informačnej bezpečnosti; je vlastníkom procesu riadenia a zabezpečovania bezpečnosti v obci; manažér kybernetickej bezpečnosti stojí na čele Bezpečnostného výboru obce,

n) prevádzkovateľ základnej služby – orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu, ktorá závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti alebo je prvkom kritickej infraštruktúry,

o) riešenie kybernetického bezpečnostného incidentu – všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov,

p) riziko – miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,

q) sieť – prenosové systémy, ktoré môžu ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej administratívnej kapacite, prípadne prepájacie alebo smerovacie zariadenie a iné prostriedky vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných (s prepájaním okruhov a paketov vrátane internetu) a mobilných sietí, elektrických káblových systémov v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na typ prenášaných informácií,

r) služba – poskytované služby obcou, výpočtové a komunikačné služby a pod. (poskytovaná funkcionalita vytvorená jedným alebo viacerými informačnými systémami),

o) základná služba – služba, ktorá je zaradená v zozname základných služieb v zmysle zákona o kybernetickej bezpečnosti a
   - závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 k zákonu o kybernetickej bezpečnosti,
   - je informačným systémom verejnej správy alebo
   - je prvkom kritickej infraštruktúry,

p) závažný bezpečnostný incident – nežiadúca udalosť, pri ktorej existuje veľmi vysoká pravdepodobnosť ohrozenia bezpečnosti (dostupnosti, dôvernosti a integrity) informácií obce, a ktorá má významné dopady na bezpečnosť alebo prevádzku kritických informačných systémov, procesov alebo môže spôsobiť škody významného prevádzkového, finančného alebo reputačného rozsahu; o tom, či je konkrétny bezpečnostný incident závažný, rozhoduje manažér kybernetickej bezpečnosti (ďalej len „MKB“).

Článok III.
PREDMET ZMLUVY

1. V zmysle § 19 ods. 2 zákona o kybernetickej bezpečnosti a s ohľadom na zmluvu o poskytovaní služieb, je predmetom tejto Zmluvy stanovenie práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti Zmluvy o službách.
2. Konkrétny rozsah činností Dodávateľa, ktoré priamo súvisia s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby:
   a) Informačný systém Urbis,
   b) Informačný systém Envita,
   c) Zálohovací systém,
   d) Emailový systém,
   e) Kamerový systém obce,
   f) Sieťové systémy obce (metropolitné sieť obce, interná sieť pre obecný úrad).
3. Dodávateľ poskytne nevyhnutné súčinnosť Prevádzkovateľovi pri nasledovných informačných systémom Prevádzkovateľa; tie nie sú predmetom tejto zmluvy:
   a. Informačný systém Esona,
   b. Registratúra (AVRIS),
   c. Webové sídlo obce (Moderné obce).

Článok IV.
POVINNOSTI DODÁVATEĽA

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené ciele tejto Zmluvy podľa zákona o kybernetickej bezpečnosti a ostatnej platnej legislatívy. Zoznam bezpečnostných opatrení Prevádzkovateľa základnej služby a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v prílohe č. 2 k tejto Zmluve.
2. Dodávateľ sa zaväzuje:
   a) poskytnúť Dodávateľovi súčinnosť pri výkone činností uvedených v § 19 ods. 6 zákona o kybernetickej bezpečnosti,
   b) prijať opatrenia v rozsahu vyhlášky č. 362/2018 Z. z. a § 20 zákona o kybernetickej bezpečnosti,
   c) plniť povinnosti týkajúce sa kybernetickej bezpečnosti Prevádzkovateľa základnej služby,
   d) zdokumentovať prijaté bezpečnostné opatrenia najmenej v rozsahu stanovenom § 20 zákona o kybernetickej bezpečnosti.
3. Dodávateľ vyhlasuje, že súhlasí so stanovenými bezpečnostnými opatreniami uvedenými v tejto Zmluve.
4. Dodávateľ je zároveň povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby, s ktorými ho Prevádzkovateľ základnej služby písomne oboznámil prostredníctvom školenia, ktoré zabezpečí Prevádzkovateľ základnej služby do 14 dní odo dňa účinnosti tejto Zmluvy. Na záver školenia podľa predchádzajúcej vety osoby poverené Dodávateľom podpíšu čestné prehlásenie o tom, že sa oboznámili s bezpečnostnými politikami Prevádzkovateľa základnej služby a že s nimi súhlasia. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa základnej služby.
5. Dodávateľ súhlasí s tým, že bezpečnostné politiky Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných

systémov Prevádzkovateľa základnej služby a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby. Prevádzkovateľ základnej služby je povinný bezodkladne písomne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené 14 dní pred ich implementáciou, pričom Dodávateľ následne písomne potvrdí oboznámenie sa so zmenenou bezpečnostnou politikou. Takéto potvrdenie je oprávnená podpísať kontaktná osoba Dodávateľa.

6. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 k tejto Zmluve.
7. Dodávateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto Zmluvy.
8. Odplata za plnenie povinností Dodávateľa podľa tejto Zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto Zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom základnej služby Dodávateľovi podľa zmluvy o poskytovaní služieb a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto Zmluvy od Prevádzkovateľa základnej služby nemá nárok.
9. Dodávateľ sa zaväzuje, že nezapojí ďalšieho dodávateľa (ďalej len „subdodávateľ“) úplne alebo čiastočne zabezpečujúceho plnenie tejto Zmluvy predtým, než dostane písomný súhlas Prevádzkovateľa základnej služby. Zoznam subdodávateľov tvorí prílohu č. 3 k tejto Zmluve. Dodávateľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Dodávateľa uvedené v tejto Zmluve. Dodávateľ je plne zodpovedný voči Prevádzkovateľovi základnej služby za plnenie povinností subdodávateľa.
10. Plnenie povinností podľa tejto Zmluvy tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Prevádzkovateľa základnej služby podľa zmluvy o poskytovaní služieb. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto Zmluvy po celú dobu trvania zmluvy o poskytovaní služieb.

## Článok V.
## BEZPEČNOSTNÉ OPATRENIA

1. Dodávateľ je povinný vykonávať činnosti v tejto Zmluve v súlade s platnými právnymi predpismi. V prípade, že Dodávateľ v rámci servisných zásahov bude využívať vzdialený prístup do počítačovej siete Prevádzkovateľa základnej služby, musí postupovať podľa ustanovení uvedených v prílohe č. 2 k tejto Zmluve.
2. Dodávateľ sa zaväzuje, že má zavedené a implementované bezpečnostné opatrenia v súlade s ustanovením § 20 ods. 3 zákona o kybernetickej bezpečnosti minimálne v rozsahu:
   a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
   b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
   c) personálnej bezpečnosti,
   d) riadenia prístupov,
   e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
   f) bezpečnosti pri prevádzke informačných systémov a sietí,
   g) hodnotenia zraniteľností a bezpečnostných aktualizácií,
   h) ochrany proti škodlivému kódu,

i) sieťovej a komunikačnej bezpečnosti,
j) akvizície, vývoja a údržby informačných sietí a informačných systémov,
k) zaznamenávania udalostí a monitorovania,
l) fyzickej bezpečnosti a bezpečnosti prostredia,
m) riešenia kybernetických bezpečnostných incidentov,
n) kryptografických opatrení,
o) kontinuity prevádzky,
p) auditu, riadenia súladu a kontrolných činností.

3. Bezpečnostné opatrenia musia v súlade s ustanovením § 20 ods. 4 zákona o kybernetickej bezpečnosti zahŕňať najmenej:
   - detekciu kybernetických bezpečnostných incidentov,
   - evidenciu kybernetických bezpečnostných incidentov,
   - postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
   - určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
   - prepojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.
4. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu v organizácii.
5. Obsah a štruktúra bezpečnostnej dokumentácie v súlade s ustanovením § 2 ods. 1 vyhlášky č. 362/2018 Z.z.:
   - schválená bezpečnostná stratégia kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,
   - klasifikácia informácií a kategorizácia sietí a informačných systémov,
   - zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
   - vykonaná analýza rizík kybernetickej bezpečnosti,
   - záverečná správa o výsledkoch auditu kybernetickej bezpečnosti v súlade s ustanovením § 29 zákona o kybernetickej bezpečnosti.
6. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby, najmä chrániť ich integritu, dôvernosť a dostupnosť pri ich spracúvaní a nakladaní s nimi.
7. V oblasti technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa §9 vyhlášky č. 362/2018 Z. z., najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Prevádzkovateľa základnej služby a ktoré toto poskytovanie služieb Prevádzkovateľa základnej služby ovplyvňujú napríklad prostredníctvom opatrení definovaných v nasledujúcich bodoch alebo opatrí s porovnateľným účinkom:
   - Zavedenie a prevádzka nastroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou služieb poskytovaných podľa zmluvy o poskytovaní služieb.
   - Zavedenie a prevádzka nastroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich času, ak sú súčasťou služieb poskytovaných podľa zmluvy o poskytovaní služieb.
   - Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

9. Dodávateľ je ďalej povinný:
   - zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa základnej služby,
   - sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
   - zasielať Prevádzkovateľovi základnej služby včasné varovania pred bezpečnostnými incidentami, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak.
   - spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby,
   - po skončení zmluvy o poskytovaní služieb vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má Prevádzkovateľ základnej služby počas plnenia zmluvy o poskytovaní služieb prístup, okrem prípadov, ak z osobitných právnych predpisov vyplýva opak,
   - prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, 10, 12. 14 a 15 vyhlášky č. 362/2018 Z. z. a v rozsahu špecifikovanom v Bezpečnostnej politike kybernetickej bezpečnosti a informačnej bezpečnosti Prevádzkovateľa základnej služby.

## Článok VI.
## PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby (ďalej len „incidenty"):
   a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa základnej služby,
   b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore a tejto Zmluvy alebo budú mať prístup k informáciám Prevádzkovateľa základnej služby,
   c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
   d) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
   e) predchádzať vzniku incidentov,
   f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
   g) prijímať od Prevádzkovateľa základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
   h) zasielať Prevádzkovateľovi základnej služby včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak a
   i) spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby.

2. Dodávateľ sa zaväzuje počas trvania tejto Zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto Zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto Zmluvy.
3. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí sa budú podieľať na plnení zmluvy o poskytovaní služieb a tejto Zmluvy a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby, je uvedený v prílohe č. 1 k tejto Zmluve. Dodávateľ je povinný písomne oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení a to bezodkladne po tom, ako táto zmena v personálnom obsadení nastane; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení podľa tohto bodu. Dodávateľ je povinný uvedenú povinnosť Prevádzkovateľovi základnej služby kedykoľvek na požiadanie preukázať.
4. Dodávateľ sa zaväzuje stanoviť postupy plnenia svojich povinností podľa tejto Zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi základnej služby na nahliadnutie a zhotovenie kópií.
5. Dodávateľ sa zaväzuje prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN ISO/IEC 27002:2022 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti) v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
6. Dodávateľ sa zaväzuje prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. d) g), h), i) k) a m) zákona o kybernetickej bezpečnosti v rozsahu podľa §8, 11, 12, 13, 15 a 17 vyhlášky č. 362/2018 Z. z. a v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
7. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

## Článok VII.
## POSTUP PRI RIEŠENÍ KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý kybernetický bezpečnostný incident, ako aj všetky ďalšie informácie požadované Prevádzkovateľom základnej služby na plnenie jeho povinností vplývajúcich zo zákona o kybernetickej bezpečnosti a informácie majúce vplyv na Zmluvu ako aj zmluvu o poskytovaní služieb Prevádzkovateľovi základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov. Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Hlásenie kybernetického bezpečnostného incidentu kategórie I. podľa prílohy č. 1 k vyhláške Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritéria pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (ďalej len „vyhláška č. 165/2018 Z. z.), nahlasuje Dodávateľ elektronicky na e-mailovú adresu MKB, hlásenie kybernetického bezpečnostného incidentu kategórie II. a III. podľa prílohy č. 1 k vyhláške č. 165/2018 Z. z. nahlasuje Dodávateľ telefonicky a zároveň elektronicky na e-mailovú adresu MKB na kontakty uvedené v prílohe č. 1 k tejto Zmluve. Ohlasovanie ďalších informácii informácií požadovaných Prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo

zákona o kybernetickej bezpečnosti a informácií majúcich vplyv na zmluvu. Dodávateľ ohlasuje písomne na adresu Prevádzkovateľa základnej služby uvedenú v záhlaví tejto Zmluvy alebo elektronicky na e-mailovú adresu MKB, ako aj SMS na telefónne číslo MKB, na kontakt uvedený v prílohe č. 1 k tejto Zmluve.

3. Dodávateľ sa po detekcii kybernetického bezpečnostného incidentu zaväzuje riešiť kybernetické bezpečnostné incidenty najmä odozvou alebo inou reakciou na kybernetický bezpečnostný incident, ohraničením kybernetického bezpečnostného incidentu a jeho dopadov, nápravou následkov kybernetického bezpečnostného incidentu, asistenciou pri riešení kybernetického bezpečnostného incidentu na mieste, reakciou na kybernetický bezpečnostný incident a podporou reakcií na kybernetický bezpečnostný incident (ďalej len „reaktívne opatrenie"). Pri riešení kybernetických bezpečnostných incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického bezpečnostného incidentu.
4. Dodávateľ sa zaväzuje v čase detekcie kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby.
5. Dodávateľ sa zaväzuje oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
6. Dodávateľ sa zaväzuje oznámiť bezodkladne, ale najneskôr do 24 hodín po detekcii kybernetického bezpečnostného incidentu oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s kybernetickým bezpečnostným incidentom mohlo dôjsť k spáchaniu trestného činu.
7. Dodávateľ sa zaväzuje bezodkladne, ale najneskôr do 24 hodín po detekcii kybernetického bezpečnostného incidentu oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.
8. Po vyriešení kybernetického bezpečnostného incidentu je Dodávateľ na výzvu Prevádzkovateľa základnej služby v určenej lehote definovanej vo výzve povinný predložiť Prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „bezpečnostné opatrenia") na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom základnej služby na jeho návrhu.
9. Po schválení bezpečnostného opatrenia Prevádzkovateľom základnej služby, je Dodávateľ povinný bezpečnostné opatrenie bez zbytočného odkladu, najneskôr však v lehote do 3 pracovných dní, vykonať. Výnimku po opodstatnenom odôvodnení písomne schvaľuje poverený zástupca prevádzkovateľa (kontakty uvedené v prílohe č. 1). Po vykonaní bezpečnostného opatrenia Dodávateľom, je Dodávateľ povinný za prítomnosti MKB Poskytovateľa základnej služby preveriť jeho efektívnu účinnosť. Zmluvné strany sa dohodli, že účinnosť bezpečnostných opatrení bude podmienená výkonom simulovaných útokov, pričom záver takýchto simulovaných útokov bude vyhodnotený na základe protokolu o efektívnom účinku ochranného opatrenia za Prevádzkovateľa základnej služby písomne schválenom MKB a za Dodávateľa písomne schváleným oprávnenou osobou, resp. kontakty uvedené v prílohe č. 1.

## Článok VIII.
## ZÁVÄZOK MLČANLIVOSTI

1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy o poskytovaní služieb, a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti. Dodávateľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby. Dodávateľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Dodávateľovi.
2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto Zmluvy, resp. zmluvy o poskytovaní služieb.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.
4. Dodávateľ sa zaväzuje zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu, obchodného vzťahu alebo iného vzťahu.
5. Po ukončení tejto Zmluvy, resp. zmluvy o poskytovaní služieb je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto Zmluvy prístup, resp. tieto podľa pokynu Prevádzkovateľa základnej služby zničiť.

## Článok IX.
## POVINNOSTI PO SKONČENÍ ZMLUVY

1. Po ukončení tejto Zmluvy je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto Zmluvy prístup, resp. tieto podľa pokynu Prevádzkovateľa základnej služby zničiť.
2. Zmluvné strany berú na vedomie, že predmetom plnenia zmluvy o poskytovaní služieb môže byť môže byť autorské dielo podľa zákona č. 185/2015 Z. z. Autorský zákon v platnom znení, ktorého súčasťou môže byť:
   a) softvér, ktorý bol vytvorený Dodávateľom predovšetkým pre podmienky a potreby Prevádzkovateľa základnej služby;
   b) softvér Dodávateľa, ktorý má všeobecný charakter;
   c) softvér tretích osôb; alebo
   d) Open Source softvér, ktorý je podriadený príslušnej licencii slobodného softvéru.
3. Zmluvné strany berú ďalej na vedomie, že predmetom plnenia zmluvy o poskytovaní služieb môže byť aj vytvorenie alebo poskytnutie iných predmetov duševného vlastníctva, ako sú napr. technická a užívateľská dokumentácia, prevádzkový manuál, návrh riešenia k Softvéru alebo k Balíkovému softvéru alebo konkrétne digitálne dizajny, vrátane grafického užívateľského rozhrania (GUI), jednotlivých ikon či symbolov, prípadne konkrétne know-how Dodávateľa.
4. S ohľadom na body 1, 2 a 3 tohto článku IX. Zmluvy zmluvné strany berú na vedomie, že Dodávateľ je v zmysle § 8 ods. 2 písm. p) vyhlášky č. 362/2018 Z. z. povinný po zániku Zmluvy umožniť Prevádzkovateľovi základnej služby zabezpečiť kontinuitu prevádzkovanej základnej služby vo vzťahu k službám, ktoré priamo súvisia s prevádzkou tejto základnej služby v rámci sietí a informačných systémov Prevádzkovateľa základnej služby.

## Článok X.
## ZODPOVEDNOSŤ ZA ŠKODU

1. Zmluvná strana zodpovedá za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinnosti zmluvnej strany stanovenej zákonom o kybernetickej bezpečnosti, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvou. Za škodu vzniknutú zmluvnej strane sa na účely Zmluvy nepovažuje pokuta alebo akákoľvek iná sankcia uložená zmluvnej strane príslušným štátnym orgánom.
2. V prípade, ak v dôsledku porušenia zákona o kybernetickej bezpečnosti alebo porušenia povinností vyplývajúcich z tejto Zmluvy na strane Dodávateľa vznikne Prevádzkovateľovi základnej služby ujma alebo finančná sankcia, Dodávateľ zodpovedá za spôsobenú škodu podľa ustanovení zákona o kybernetickej bezpečnosti. V prípade sankcie uloženej Národným bezpečnostným úradom, túto znáša v plnom rozsahu Dodávateľ.
3. V prípade, že zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo zákonom o kybernetickej bezpečnosti, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvy (ďalej ako „porušujúca zmluvná strana“) a v dôsledku tohto konania alebo opomenutia konania porušujúcej zmluvnej strany preukázateľne dôjde k vzniku škody na strane druhej zmluvnej strany (ďalej ako „poškodená zmluvná strana“), zaväzuje sa porušujúca zmluvná strana túto škodu vzniknutú poškodenej zmluvnej strane nahradiť.
4. Vznik zodpovednosti porušujúcej zmluvnej strany za škodu vzniknutú poškodenej zmluvnej strane je však podmienená povinnosťou poškodenej zmluvnej strany preukázať porušujúcej zmluvnej strane existenciu príčinnej súvislosti medzi porušením povinnosti podľa Zmluvy alebo zákona o kybernetickej bezpečnosti, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy na strane porušujúcej zmluvnej strany a vznikom škody. Príčinná súvislosť nie je okrem iného daná aj vtedy, ak porušujúca zmluvná strana nesplnila svoju všeobecnú preventívnu povinnosť počínať si tak, aby nedochádzalo ku vzniku škôd. Počínaním podľa predchádzajúcej vety sa rozumie najmä akýkoľvek postup zmluvnej strany, na ktorý je v zmysle Zmluvy alebo zákona o kybernetickej bezpečnosti, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy oprávnená a prostredníctvom ktorého mohlo byť vzniku škody zabránené.
5. V prípade preukázania existencie príčinnej súvislosti podľa tohto ustanovenia článku X. Zmluvy je porušujúca zmluvná strana povinná uhradiť poškodenej zmluvnej strane vzniknutú škodu, a to v lehote do 10 dní odo dňa doručenia na základe písomnej výzvy poškodenej Zmluvnej strany doručenej porušujúcej zmluvnej strane na adresu uvedenú v záhlaví tejto Zmluve, alebo na inú porušujúcou Zmluvnou stranou oznámenú adresu.
6. Zánikom tejto Zmluvy nie sú dotknuté tie ustanovenia, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zániku tejto Zmluvy a záväzky na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy.

## Článok XI.
## KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Dodávateľ sa zaväzuje komunikovať pri plnení povinností podľa tejto Zmluvy s Prevádzkovateľom základnej služby spôsobom určeným Prevádzkovateľom základnej služby, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 k tejto Zmluve.

3. Dodávateľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 k tejto Zmluve.
4. Kontaktné osoby podľa prílohy č. 1 k tejto Zmluve môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia tejto Zmluvy o doručovaní.

## Článok XII.
## SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi ako aj ostatnej platnej legislatívy, vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.
2. Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy na zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
4. Dodávateľ sa zaväzuje dokumentovať svoju činnosť podľa tejto Zmluvy (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť Prevádzkovateľa základnej služby mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
5. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy bezodkladne, pokiaľ to nie je v tejto Zmluve alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
6. V prípade, ak Dodávateľ plní Zmluvu prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby, Dodávateľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto Zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto Zmluvy. Dodávateľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto Zmluvy aj u týchto subdodávateľov.
7. Akékoľvek oznámenia zmluvných strán podľa tejto Zmluvy realizované formou e-mailu sa považujú za doručené druhej zmluvnej strane nasledujúci pracovný deň po dni, kedy bolo odosielateľovi preukázateľne odoslané potvrdenie o doručení e-mailu adresátovi bez ohľadu na to, či došlo k prečítaniu správy na strane adresáta, s tým, že v prípade detekcie kybernetického bezpečnostného incidentu a povinností Dodávateľa spojených s jeho hlásením Prevádzkovateľovi základnej služby je podmienené aj odoslaním SMS MKB podľa ust. čl. VII ods. 2 Zmluvy.
8. Komunikácia, majúca vplyv na zmenu alebo zánik tejto Zmluvy bude uskutočnená písomnou formou. Písomné podanie sa považuje za riadne uskutočnené, ak bolo podané na poštovú prepravu alebo doručené osobne na

adresu sídla druhej zmluvnej strany uvedenú v záhlaví Zmluvy, prípadne na inú adresu písomne oznámenú druhou zmluvnou stranou.

9. Ak sa podanie odoslané prostredníctvom pošty vráti odosielateľovi späť s vyznačením adresát neznámy alebo adresát neprevzal v odbernej lehote, bude sa podanie považovať za doručené v deň jeho vrátenia odosielateľovi, a to bez ohľadu na to, či sa s podaním zmluvná strana oboznámila alebo nie, ak nie je doručenie podania preukázané skôr.
10. Ak zmluvná strana bezdôvodne odoprie prijať doručovanú písomnosť, považuje sa písomnosť za doručenú dňom, keď prijatie písomnosti bolo odopreté.
11. V prípade, ak Dodávateľ spôsobí Prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo Zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov. Pre odstránenie právnych pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.
12. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej zmluvnej strane (ďalej len „písomnosti“) musia byť doručené, ak Zmluva neustanovuje inak:
    a) v písomnej forme prostredníctvom pošty doporučene s doručenkou; za deň doručenia sa považuje dátum prevzatia zásielky alebo
    b) osobne do sídla druhej zmluvnej strany.
13. Miestom pre doručovanie písomností sú adresy zmluvných strán uvedené v záhlaví tejto Zmluvy. Každá zo zmluvných strán je povinná písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu ohľadne doručovania, a to najneskôr do 5 pracovných dní po tom, čo k takejto zmene dôjde. Pokiaľ sa z dôvodu oneskoreného alebo nevykonaného oznámenia o zmene miesta doručovania nepodarí včas a riadne doručiť písomnosť druhej zmluvnej strane, považuje sa deň neúspešného pokusu o opakované doručenie písomnosti za deň doručenia písomnosti druhej zmluvnej strane so všetkými právnymi dôsledkami pre dotknutú zmluvnú stranu.
14. Dodávateľ sa zaväzuje oznamovať všetky skutočnosti majúce vplyv na Zmluvu, ako aj hlásiť ďalšie informácie požadované Prevádzkovateľom základnej služby, písomne na adresu sídla Prevádzkovateľa základnej služby.

## XIII.
## VYŠŠIA MOC

1. Vyššia moc znamená mimoriadnu udalosť alebo okolnosť, ktorú nemohla žiadna zo zmluvných strán pred uzatvorením Zmluvy predvídať, ktorá je mimo kontroly ktorejkoľvek zo zmluvných strán a nebola spôsobená úmyselne alebo z nedbanlivosti konaním alebo opomenutím ktorejkoľvek zmluvnej strany a ktorá podstatným spôsobom sťažuje alebo znemožňuje plnenie povinností podľa Zmluvy ktoroukoľvek zo zmluvných strán. Takýmito udalosťami alebo okolnosťami sú najmä, nie však výlučne, vojna, teroristický útok, občianske nepokoje, vzbura, pandémia závažného život ohrozujúceho nákazlivého ochorenia, prítomnosť ionizujúceho alebo rádioaktívneho žiarenia, požiar, výbuch, povodeň či iné živelné pohromy alebo prírodné katastrofy. Výslovne sa stanovuje, že Vyššou mocou nie je štrajk personálu Dodávateľa ani hospodárske pomery zmluvných strán.
2. Ak niektorej zo zmluvných strán bráni alebo bude brániť v plnení niektorej jej povinnosti podľa Zmluvy vyššia moc, potom písomne oznámi druhej zmluvnej strane udalosť alebo okolnosti, ktoré predstavujú vyššiu moc,

uvedie povinnosti, v ktorých plnení jej vyššia moc bráni alebo bude brániť a predpokladané trvanie takej okolnosti predstavujúcej vyššiu moc. Oznámenie musí byť urobené bezodkladne, najneskôr však v lehote 3 dní potom, čo sa zmluvná strana dozvedela alebo sa pri vynaložení riadnej odbornej starostlivosti mala a mohla dozvedieť o príslušnej udalosti alebo okolnostiach predstavujúcich dôvod vyššej moci. Ak je to možné, pri vynaložení riadnej odbornej starostlivosti, musí uvedené oznámenie obsahovať návrh opatrení vedúcich k zmierneniu alebo vylúčeniu dôsledkov okolností predstavujúcich vyššiu moc. V ostatných prípadoch bude oznámenie obsahovať iba najbližší možný termín, do ktorého môže byť návrh opatrenia poskytnutý pri vynaložení primeraného úsilia. Ak návrh opatrenia druhá zmluvná strana schváli, na čo má lehotu 3 dní, postupuje zmluvná strana dotknutá vyššou mocou podľa neho až do ukončenia okolností vyššej moci.

3. Po uskutočnení tohto oznámenia príslušnou zmluvnou stranou, nebude táto zmluvná strana zodpovedná za príslušné porušenia povinností po dobu, dokiaľ jej vyššia moc bráni alebo bude brániť v ich plnení.
4. Zmluvnú stranu nezbavuje zodpovednosti za porušenie povinnosti vyššia moc, ktorá nastala až v čase, kedy bola povinná zmluvná strana v omeškaní s plnením jej povinnosti. Účinky vylúčenia zodpovednosti sú obmedzené iba na dobu, dokiaľ trvá vyššia moc.
5. Každá zmluvná strana vždy vyvinie všetko úsilie potrebné k tomu, aby minimalizovala omeškanie pri plnení svojich povinností podľa zmluvy, ktoré vzniklo v dôsledku vyššej moci, najmä plniť návrh opatrenia, ak je tento schválený druhou zmluvnou stranou.
6. Príslušná Zmluvná strana oznámi druhej zmluvnej strane okamih ukončenia pôsobenia vyššej moci v rovnakej lehote ako pri oznámení o jej vzniku podľa bodu 2 tohto článku tejto Zmluvy.
7. Ak je z dôvodu okolnosti vylučujúcej zodpovednosť alebo prípadu vyššej moci plnenie Zmluvy jednej zo zmluvných strán ovplyvnené len čiastočne, takáto zmluvná strana zostáva zodpovedná za plnenie tých záväzkov, ktoré okolnosťou vylučujúcou zodpovednosť alebo vyššou mocou nie sú dotknuté.
8. Ak má niektorý zo subdodávateľov podľa akejkoľvek zmluvy či dohody týkajúcej sa poskytovania služby podľa tejto Zmluvy širšie definovaný nárok na omeškanie v dôsledku pôsobenia vyššej moci, okolností vylučujúcich zodpovednosť alebo iného obdobného právneho inštitútu, než ako je definovaná vyššia moc podľa tejto Zmluvy, takéto širšie definované udalosti alebo okolnosti neospravedlňujú porušenie povinností podľa Zmluvy s Dodávateľom ani mu nezakladajú nároky podľa tohto článku Zmluvy.
9. Ak účinky Vyššej moci trvajú nepretržite viac ako 5 dní je príslušná zmluvná strana oprávnená odstúpiť od tejto Zmluvy podľa článku XV. ods. 2 písm. d) tejto Zmluvy.

## Článok XIV.
## AUDIT KYBERNETICKEJ BEZPEČNOSTI

1. Prevádzkovateľ základnej služby je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy.
2. Dodávateľ je povinný predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.
3. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.

4. Prevádzkovateľ základnej služby môže audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
5. Dodávateľ sa zaväzuje pri audite spolupracovať s Prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
6. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
7. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi základnej služby súlad s touto Zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
8. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej desať pracovných dní vopred svoj zámer realizovať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto Zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
10. Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe.
11. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „BOZP") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO"), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ.
12. Dodávateľ sa zaväzuje preukázateľne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia, vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

## Článok XV.
## ZÁVEREČNÉ USTANOVENIA

1. Táto Zmluva sa uzatvára na dobu určitú, a to na dobu trvania zmluvy o poskytovaní služieb.
2. Prevádzkovateľ základnej služby je oprávnený od tejto Zmluvy písomne odstúpiť v prípadoch:
   a) podstatného porušenia tejto Zmluvy zo strany Dodávateľa;
   b) ak je na Dodávateľa vyhlásený konkurz, alebo bola povolená reštrukturalizácia, alebo ak bolo vyhlásenie konkurzu odmietnuté alebo zrušené pre nedostatok majetku;

c) ak je Dodávateľ v likvidácii,
d) v prípade pretrvávania vyššej moci v zmysle čl. XIII ods. 9 Zmluvy.

3. Odstúpenie od tejto Zmluvy je platné a účinné dňom preukázateľného doručenia písomného odstúpenia od tejto Zmluvy Dodávateľovi.
4. Za podstatné porušenie tejto Zmluvy sa považuje:
   a) porušenie povinností Dodávateľom uvedených v tejto Zmluve;
   b) konanie Dodávateľa, ktorý už v čase uzavretia Zmluvy vedel alebo v tomto čase mohol predvídať s prihliadnutím na účel Zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola Zmluva uzavretá, že nedodrží, poruší a/alebo nebude plniť zmluvnú povinnosť dojednanú touto Zmluvou a to bez ohľadu na to, či ide o zmluvnú povinnosť uvedenú v predchádzajúcom písm. a) a je zrejmé, že Prevádzkovateľ základnej služby by nemal záujem uzatvoriť túto Zmluvu pri takom porušení Zmluvy;
5. Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto Zmluvy.
6. Túto Zmluvu je možné vypovedať Prevádzkovateľom základnej služby písomnou výpoveďou, aj bez uvedenia dôvodu s výpovednou dobou 1 mesiac, ktorá začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená Dodávateľovi.
7. Zmluvné strany sa dohodli, že túto Zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán. V tomto prípade Zmluva zaniká ku dňu, ktorý bude v tejto dohode určený ako deň zániku Zmluvy. Ak takýto deň určený nie je, táto Zmluva zaniká ku dňu nadobudnutia účinnosti takejto dohody.
8. Zrušenie tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zrušení tejto Zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy.
9. Po ukončení tejto Zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovania základnej služby na Prevádzkovateľa základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto Zmluvy.
10. Táto Zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy výslovne neupravené touto Zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
11. Prípadné spory vyplývajúce z tejto Zmluvy budú riešené predovšetkým mimosúdne. Podpisom tejto Zmluvy zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto Zmluvy sú príslušné súdy Slovenskej republiky.
12. Táto Zmluva sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo zmluvy nevyplýva niečo iné.
13. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto Zmluvy na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
14. Ak niektoré ustanovenia tejto Zmluvy budú zmluvné strany, súd alebo iné kompetentné orgány považovať za neplatné alebo nevymáhateľné, potom takéto ustanovenie bude neplatné iba v dotknutom a v najužšom možnom rozsahu, pričom jeho zvyšná časť, význam a dopady, ako aj ostatné ustanovenia tejto Zmluvy zostávajú v platnosti. Zmluvné strany budú v takom prípade postupovať tak, aby účel ustanovení považovaných za nevymáhateľné alebo neplatné bol v maximálne možnej miere rešpektovaný a pre zmluvné strany právne záväzný vo forme umožňujúcej jeho právnu vymáhateľnosť.
15. Táto Zmluva tvorí úplnú dohodu medzi zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto Zmluvy zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto Zmluvy a žiadna

zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto Zmluve neuvedených, ústnych alebo písomných dojednaní a dohôd.

16. Táto Zmluva je vyhotovená v štyroch rovnopisoch, a to v dvoch rovnopisoch pre Prevádzkovateľa základnej služby a vo dvoch rovnopisoch pre Dodávateľa.
17. Zmluvné strany berú na vedomie, že Prevádzkovateľ základnej služby je v zmysle § 2 ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov povinnou osobou a preto je táto Zmluva v zmysle § 5a tohto zákona v spojení s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov povinne zverejňovanou zmluvou.
18. Táto Zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR.
19. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.
20. Neoddeliteľnou súčasťou tejto Zmluvy sú jej prílohy:
    - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa,

V Bernolákove, dňa 28.7.2025

| | |
|---|---|
| Prevádzkovateľ základnej služby | Dodávateľ |
| Obec Bernolákovo | ESKAVER, s.r.o. |
| Ing. Miroslav Turenič, MBA, LL.M. | Andrea Belanová |
| starosta obce | konateľ |

Príloha č. 1 Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a dodávateľa (vzor)

Prevádzkovateľ základnej služby:

| | |
|---|---|
| Meno a priezvisko: | JUDr. Juraj Ďorko, PhD. |
| Rola/pozícia: | Prednosta obecného úradu |
| Proces súvisiaci s prevádzkou ZS; popis vykonávaných činností: | Správa serverov, počítačovej a metropolitnej siete a kamerového systému obce Bernolákovo |
| Telefonický kontakt: | 02/ 40 200 610 |
| e-mail: | prednosta@bernolakovo.sk |

Dodávateľ:

| | |
|---|---|
| Meno a priezvisko: | Andrej Koška |
| Rola/pozícia: | IT manager |
| Proces súvisiaci s prevádzkou ZS; popis vykonávaných činností: | Správa serverov, počítačovej a metropolitnej siete a kamerového systému obce Bernolákovo |
| Telefonický kontakt: | 0918 727 909 |
| e-mail: | koska@eskaver.sk |