ZMLUVA
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

podľa § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení (ďalej ako „**Zákon**“) medzi zmluvnými stranami:

Obchodné meno:	**Mesto Galanta**
Sídlo:	Mierové námestie č. 940/1
IČO:	00305936
Zápis v registri:	

(ďalej ako „**Prevádzkovateľ základnej služby**“ alebo ako „**Zmluvná strana**“)

a

Obchodné meno:	**NOVITECH Nové Zámky, s.r.o.**
Sídlo:	Komárňanská cesta 1, 940 64 Nové Zámky
IČO:	34104445
Zápis v registri:	Obchodný register Okresného súdu Nitra, Oddiel Sro, vložka č. 407/N

(ďalej ako „**Tretia strana**“ alebo ako „**Zmluvná strana**“)

(Prevádzkovateľ základnej služby a Tretia strana ďalej spolu aj ako „**Zmluvné strany**“)

PREAMBULA

*NAKOĽKO Prevádzkovateľ základnej služby s Treťou stranou uzatvoril Zmluvy o poskytovaní IT služieb (ďalej ako „**Hlavná zmluva**“), ktorá určuje obsah a rozsah plnenia poskytovaného Treťou stranou Prevádzkovateľovi základnej služby, ktorým (plnením) je **vytvorenie virtuálnej infraštruktúry v prostredí Microsoft AZURE a jej nastavenie** podľa Hlavnej zmluvy (ďalej ako „**Plnenie**“);*

NAKOĽKO Zmluvné strany vyhlasujú, že Plnenie poskytované Treťou stranou priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa základnej služby, v dôsledku čoho je daná povinnosť v zmysle § 19 ods. 2 Zákona uzatvoriť s Treťou stranou zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti Zmluvy;

*NAKOĽKO Zmluvné strany vyhlasujú, že pred uzatvorením tejto zmluvy bola vykonaná analýza rizík podľa bodu 1.2 tejto zmluvy vo vzťahu dodávateľskému vzťahu a k Plneniu v súlade s § 6 Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z .z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v platnom znení (ďalej ako „**Vyhláška**“);*

zmluvné strany uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej ako „**Zmluva**“) s nasledovným znením:

Článok 1
Úvodné ustanovenia

1.1 Ak Zmluva výslovne neustanovuje inak, všetky pojmy uvedené v Zmluve majú význam, aký im priznáva Zákon, Vyhláška, iný aplikovateľný všeobecne záväzný právny predpis, Zmluva alebo Hlavná zmluva. V prípade rozporov vo výklade niektorého z pojmu uvedeného v Zmluve platí nasledovná hierarchia aplikácie výkladu pojmu v poradí od výkladu s najvyššou prioritou po výklad s najnižšou prioritou:

1.1.1 Zákon;
1.1.2 Vyhláška;
1.1.3 iný aplikovateľný všeobecne záväzný právny predpis;
1.1.4 Zmluva; a
1.1.5 Hlavná zmluva.

Pre vylúčenie akýchkoľvek pochybností platí, že na výklad obsahu pojmu uvedeného v Zmluve sa prednostne použije výklad v zmysle Zákona, pričom v prípade, ak takýto výklad v Zákone absentuje, použije sa výklad podľa bodu 1.1.2 Zmluvy, príp. ďalšieho z bodov 1.1.3 až 1.1.5 Zmluvy. V prípade, pokiaľ nebude možné identifikovať výklad konkrétneho pojmu použitého v Zmluve ani podľa jedného z bodov 1.1.1 až 1.1.5 Zmluvy, použije sa výklad pojmu s takým významom, v akom bol prvý krát použitý v Zmluve.

1.2 V súlade s § 9 ods. 1 Vyhlášky pri uzatvorení zmluvy s Treťou stranou podľa § 19 ods. 2 Zákona, a teda pri uzatvorení Zmluvy boli analyzované riziká spojené s dodávateľským vzťahom medzi Zmluvnými stranami a Plnením spôsobom podľa § 6 Vyhlášky (ďalej ako „**Analýza rizík**"). Výstup z analýzy rizík (identifikácia rizík a ich kvalifikácia alebo kvantifikácia) tvorí ***Prílohu č. 1*** Zmluvy. Analýzou rizík boli identifikované najmä:

1.2.1 hrozby;
1.2.2 zraniteľnosti;
1.2.3 pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou;
1.2.4 riziká s ohľadom na aktíva;
1.2.5 riziko a jeho kvalifikácia alebo kvantifikácia;
1.2.6 funkčný dopad;
1.2.7 návrh bezpečnostných opatrení v zmysle Vyhlášky v kontexte identifikovaných rizík; a
1.2.8 vlastník rizika.

1.3 Tretia strana vyhlasuje a súhlasí, že bude dodržiavať všetky interné predpisy Prevádzkovateľa základnej služby, najmä jeho bezpečnostné politiky, a to v rozsahu, v akom Prevádzkovateľ základnej služby svoje interné predpisy sprístupnil Tretej strane. To neplatí, ak príslušná povinnosť vyplýva Tretej strane zo všeobecne záväzného právneho predpisu. Povinnosť dodržiavať všetky interné predpisy Prevádzkovateľa základnej služby sa týka aj akejkoľvek úpravy, zmeny alebo doplnenia počas platnosti Zmluvy. Zmluvné strany vyhlasujú, že bezpečnostné politiky Prevádzkovateľa základnej služby, ku ktorým má Tretia strana prístup, tvoria ***Prílohu č. 2*** Zmluvy. Tretia strana zabezpečí, aby boli bezpečnostné politiky prístupné a ich obsah známy všetkým osobám podieľajúcim sa na plnení Hlavnej zmluvy a tejto Zmluvy (interní zamestnanci Tretej strany, jej subdodávatelia a pod.).

1.4 Tretia strana vyhlasuje, že má prijaté, bude dodržiavať a udržiavať všetky bezpečnostne opatrenia, ktoré sú identifikované postupom podľa bodu 1.2 Zmluvy, a to vrátane ich budúcich zmien či doplnení.

1.5 Ak sa ukáže akékoľvek vyhlásenie Zmluvnej strany podľa ustanovenia Článku 1 Zmluvy ako nepravdivé, zakladá to právo druhej Zmluvnej strany odstúpiť od tejto Zmluvy.

1.6 Zmluvné strany sa dohodli, že príslušné ustanovenia tejto Zmluvy budú vykladať s ohľadom na najnovšie platné a účinné znenie Zákona a jeho vykonávacích právnych predpisov (napr. Vyhlášky), pričom v prípade zmeny znenia Zákona alebo jeho vykonávacích právnych predpisov (vrátane doplnenia nových) nie je nevyhnutné uzatvárať dodatok k tejto Zmluve.

Článok 2
Predmet Zmluvy

2.1 Predmetom Zmluvy je úprava práv a povinností Zmluvných strán pri zabezpečovaní plnenia bezpečnostných opatrení a notifikačných povinností Treťou stranou podľa Zákona a Zmluvy pri výkone činností, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa základnej služby.

2.2 Pre účely Zmluvy sa činnosťami, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa základnej služby rozumie Plnenie poskytované Treťou stranou podľa Hlavnej zmluvy.

2.3 Zmluvné strany sa dohodli, že Prevádzkovateľ základnej služby a Tretia strana si poskytnú všetku primeranú súčinnosť pri plnení Zmluvy.

2.4 Zmluvné strany berú na vedomie a súhlasia, že aj napriek tomu, že obsah a rozsah povinností Tretej strany vo vzťahu k zabezpečeniu plnenia bezpečnostných opatrení a notifikačných povinností podľa Zmluvy je uvedený v ustanoveniach Zmluvy, ktoré je možné štandardne meniť len na základe písomných dodatkov uzatvorených oboma Zmluvnými stranami, to neplatí pre prípady zmien a doplnení bezpečnostných opatrení identifikovaných postupom podľa bodu 1.2 Zmluvy. V zmysle uvedeného platí, že Prevádzkovateľ základnej služby je oprávnený počas platnosti Zmluvy vykonať zmenu alebo doplnenie skôr identifikovaných bezpečnostných opatrení, ktoré je Tretia strana povinná v lehote identifikovanej Prevádzkovateľom základnej služby prijať. Povinnosť Tretej strany podľa predchádzajúcej vety je daná za predpokladu, pokiaľ potreba zmeny alebo doplnenia bezpečnostných opatrení vyplynie z nových alebo aktualizovaných rizík identifikovaných Prevádzkovateľom základnej služby postupom podľa § 6 Vyhlášky.

2.5 Pre vylúčenie pochybností platí, že oprávnenie Prevádzkovateľa základnej služby udeľovať Tretej strane záväzné písomné pokyny slúžiace na vykonanie príslušných ustanovení Zmluvy (vrátane platného obsahu a rozsahu bezpečnostných opatrení) nie je bodom 2.4 Zmluvy dotknuté.

Článok 3
Cena

3.1 Zmluvné strany v tejto súvislosti berú na vedomie, že uzatvorenie a plnenie Zmluvy je dôsledok legislatívnych povinností patriacich Zmluvným stranám a zároveň charakteru Plnení Tretej strany. Zmluvné strany sa preto dohodli, že cena za plnenie Zmluvy Treťou stranou je zahrnutá v cene (odplate) v zmysle Hlavnej zmluvy.

Článok 4
Subdodávateľ Tretej strany

4.1 Zmluvné strany sa dohodli, že Tretia strana je oprávnená na vlastnú zodpovednosť zapojiť ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho alebo akýmkoľvek spôsobom sa podieľajúceho na Plneniach pre Prevádzkovateľa základnej služby namiesto Tretej strany alebo spolu s Treťou stranou (ďalej ako „**Subdodávateľ**") len na základe predchádzajúceho písomného súhlasu Prevádzkovateľa základnej služby.

4.2 Tretia strana je povinná v prípade jej záujmu postupovať podľa bodu 4.1 Zmluvy a pred zapojením Subdodávateľa informovať Prevádzkovateľa základnej služby a poskytnúť mu o Subdodávateľovi požadované informácie. Prevádzkovateľ základnej služby rozhodne do 7 dní od oznámenia Tretej strany podľa predchádzajúcej vety, či so zapojením Subdodávateľa súhlasí alebo nie. V prípade, ak sa Prevádzkovateľ základnej služby v stanovenej lehote nevyjadrí, platí, že so zapojením Subdodávateľa nesúhlasí.

4.3 Tretia strana je povinná na zmluvnom základe uložiť každému Subdodávateľovi tie povinnosti Tretej strany vyplývajúce zo Zmluvy, ktoré sú primerané s ohľadom na rozsah zapojenia Subdodávateľa do Plnenia pre Prevádzkovateľa základnej služby namiesto Tretej strany alebo spolu s Treťou stranou. Pre vylúčenie pochybností platí, že Tretia strana je predovšetkým povinná pred zapojením Subdodávateľa vykonať voči Subdodávateľovi analýzu rizík podľa § 6 Vyhlášky a v nadväznosti na identifikované riziká zaviazať Subdodávateľa na prijatie a udržiavanie súvisiacich bezpečnostných opatrení v zmysle Vyhlášky. V prípade, pokiaľ Tretia strana poruší svoju povinnosť a analýzu rizík u Subdodávateľa nevykoná alebo ju vykoná v nedostatočnom rozsahu, je povinná Subdodávateľa zaviazať na prijatie a udržiavanie bezpečnostných opatrení pre všetky bezpečnostné oblasti v zmysle Vyhlášky, a to aj vtedy, pokiaľ by niektoré v prípade riadneho vykonania analýzy rizík neboli relevantné alebo potrebné.

Článok 5
Zoznam pracovných rolí

5.1 Zoznam pracovných rolí Tretej strany vrátane ich personálneho obsadenia, ktoré majú mať podľa vôle Tretej strany prístup k informáciám a údajom Prevádzkovateľa základnej služby na základe Zmluvy alebo sa akýmkoľvek spôsobom podieľať na plnení Hlavnej zmluvy alebo tejto Zmluvy, tvorí ***Prílohu č. 3*** Zmluvy. Informácie a údaje podľa tohto bodu Zmluvy majú rovnaký význam ako im priznáva Vyhláška.

5.2 Tretia strana je povinná informácie a údaje podľa tohto článku Zmluvy udržiavať aktuálne a pravdivé. Na prípadné zmeny ***Prílohy č. 3*** Zmluvy Treťou stranou sa primerane vzťahuje bod 14.1 Zmluvy

upravujúci postup pri zmene adresy Zmluvnej strany so spôsobom oznámenia tejto zmeny podľa bodu 9.5 Zmluvy.

5.3 Tretia strana je povinná dať každej osobe uvedenej v ***Prílohe č. 3*** Zmluvy alebo osobe s prístupom k informáciám a údajom Prevádzkovateľa základnej služby podpísať vyjadrenie o zachovávaní mlčanlivosti, ktoré je v súlade s § 12 ods. 1 Zákona. Povinnosť zachovávať mlčanlivosti podľa Zmluvy sa vzťahuje aj na osoby na strane Subdodávateľa.

5.4 Povinnosť zachovávať mlčanlivosť trvá aj po skončení zmluvného vzťahu s Prevádzkovateľom základnej služby, a to neobmedzene.

Článok 6
Platnosť Zmluvy a spôsob jej ukončenia

6.1 Zmluva sa uzatvára sa na dobu platnosti Hlavnej zmluvy. Vzhľadom k skutočnosti, že Zmluva sa nepovažuje za povinne zverejňovanú zmluvu podľa § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií), Zmluva nadobúda platnosť a účinnosť dňom podpisu Zmluvy oboma Zmluvnými stranami alebo poslednou z nich.

6.2 Zmluvné strany sa dohodli, že k zániku Zmluvy môže dôjsť niektorým z nasledovných spôsobov:

6.2.1 dohodou Zmluvných strán;
6.2.2 odstúpením od Zmluvy;
6.2.3 zánikom Hlavnej zmluvy.

6.3 Zmluvná strana je oprávnená odstúpiť od Zmluvy, ak tak ustanovuje Zmluva, alebo ak druhá Zmluvná strana neodstráni porušenie povinnosti podľa Zmluvy ani v časovom období 7 dní po doručení písomnej výzvy na odstránenie nedostatkov alebo závadného stavu, ktorá (výzva) bude toto porušenie špecifikovať. Oznámenie o odstúpení od Zmluvy musí byť písomné a doručené druhej Zmluvnej strane s tým, že odstúpenie od Zmluvy nadobúda účinnosť dňom doručenia tohto odstúpenia druhej Zmluvnej strane.

6.4 Zmluvné strany sa dohodli, že vzájomný vzťah Zmluvy a Hlavnej zmluvy sa riadi § 275 ods. 2 a 3 zákona č. 513/1991 Zb. Obchodný zákonník v platnom znení. V zmysle uvedeného platí, že z povahy a Zmluvným stranám známeho účelu Zmluvy pri jej uzavretí vyplýva, že Zmluva je závislá na Hlavnej zmluve. Vznik a existencia Hlavnej zmluvy je podmienkou vzniku a existencie Zmluvy. Zánik Hlavnej zmluvy spôsobuje aj zánik Zmluvy a súčasne, zánik Zmluvy spôsobuje zánik Hlavnej zmluvy, a to s obdobnými právnymi účinkami.

6.5 Vzhľadom na obsah Zmluvy je aplikácia akýchkoľvek ustanovení týkajúcich sa kybernetickej bezpečnosti podľa Zákona alebo akejkoľvek povinností Zmluvnej strany v zmysle Zákona obsiahnutých v Hlavnej zmluve vylúčená, pričom sa vždy uplatnia ustanovenia Zmluvy, ak Zmluva neustanovuje inak. Zmluvné strany svojim podpisom prehlasujú, že uvedená forma zmeny Hlavnej zmluvy podľa predchádzajúcej vety je dostačujúca a spĺňa všetky požiadavky vyžadované na platnú zmenu obsahu Hlavnej zmluvy. V prípade akýchkoľvek pochybností o aplikácii ustanovení Hlavnej zmluvy alebo Zmluvy vo vzťahu ku kybernetickej bezpečnosti alebo príslušných povinností a zodpovedností Zmluvných strán vyplývajúcich zo Zákona platí, že ustanovenia Zmluvy majú prednosť pred ustanoveniami Hlavnej zmluvy.

Článok 7
Bezpečnostné opatrenia

7.1 Bezpečnostné opatrenia sa prijímajú a dodržiavajú pre nasledovné oblasti v zmysle § 20 Zákona:

a) organizácia kybernetickej bezpečnosti a informačnej bezpečnosti;
b) riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti;
c) personálna bezpečnosť;
d) riadenie prístupov;
e) riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami;
f) bezpečnosť pri prevádzke informačných systémov a sietí;
g) hodnotenie zraniteľností a bezpečnostných aktualizácií;
h) ochrana proti škodlivému kódu;
i) sieťová a komunikačná bezpečnosť;
j) akvizícia, vývoj a údržba informačných sietí a informačných systémov;
k) zaznamenávanie udalostí a monitorovanie;
l) fyzická bezpečnosť a bezpečnosť prostredia;
m) riešenie kybernetických bezpečnostných incidentov;
n) kryptografické opatrenia;
o) kontinuita prevádzky;
p) audit, riadenie súladu a kontrolné činnosti.

7.2 Jednotlivé bezpečnostné opatrenia pre oblasti podľa bodu 7.1 Zmluvy vyplývajú z príslušného znenia Vyhlášky. Zmluvné strany berú na vedomie, že obsah povinnosti Tretej strany prijať bezpečnostné opatrenia je daný aktuálnym znením Vyhlášky, a to vrátane prípadnej zmeny či doplnenia Vyhlášky mapovaním opatrení na oblasti v zmysle § 20 ods. 3 Zákona v znení zákona č. 231/2022 Z. z., príp. neskoršieho znenia Zákona alebo Vyhlášky.

7.3 Tretia strana ako vlastník rizík podľa Analýzy rizík vyhlasuje, že prijala a bude dodržiavať a udržiavať bezpečnostné opatrenia pre tieto riziká. Konkrétna špecifikácia, obsah a rozsah bezpečnostných opatrení Tretej strany tvorí ***Prílohu č. 4*** Zmluvy. Ak z ***Prílohy č. 4*** Zmluvy nevyplýva inak, bezpečnostné opatrenia sa delia na všeobecné bezpečnostné opatrenia a bezpečnostné opatrenia reflektujúce na riziká v zmysle Analýzy rizík.

7.4 Tretia strana vyhlasuje, že počas trvania Zmluvy bude dodržiavať a udržiavať všetky bezpečnostné opatrenia podľa ***Prílohy č. 4*** Zmluvy.

Článok 8
Povinnosti Zmluvných strán

8.1 Prevádzkovateľ základnej služby je povinný Zmluvu, Hlavnú zmluvu, ako aj akúkoľvek ďalšiu zmluvnú alebo súvisiacu dokumentáciu uzatvorenú s Treťou stranou evidovať v rámci bezpečnostnej dokumentácie spôsobom podľa § 9 ods. 5 Vyhlášky.

8.2 Tretia strana je povinná chrániť všetky informácie, ktoré jej boli poskytnuté Prevádzkovateľom základnej služby pri plnení Zmluvy alebo sa do dispozície Tretej strany dostali iným spôsobom. Na tento účel je Tretia strana povinná dodržiavať mlčanlivosť a touto mlčanlivosťou zaviazať všetky

osoby, ktoré sú u Tretej strany alebo prostredníctvom Tretej strany oprávnené na prístup k informáciám Prevádzkovateľa základnej služby pri plnení Zmluvy, ak nie sú viazané povinnosťou mlčanlivosti podľa osobitného predpisu. Tretia strana vyhlasuje, že povinnosť Tretej strany chrániť informácie podľa tohto bodu Zmluvy je zabezpečená prostredníctvom vhodnej povinnosti mlčanlivosti podľa § 12 ods. 1 Zákona a bezpečnostných opatrení podľa ***Prílohy č. 4*** Zmluvy.

8.3 Prevádzkovateľ základnej služby je oprávnený požadovať od Tretej strany informácie potrebné na splnenie ktorejkoľvek povinnosti Prevádzkovateľa základnej služby vyplývajúcej zo Zákona alebo príslušnej požiadavky orgánov verejnej moci (vrátane poskytovania súčinnosti jednotkám CSIRT). Tretia strana je povinná bez zbytočného odkladu poskytnúť Prevádzkovateľovi základnej služby všetky informácie, ktoré má alebo by mala mať k dispozícii. Informácie podľa tohto bodu Zmluvy poskytuje Tretia strana bezodkladne po doručení žiadosti Prevádzkovateľa základnej služby o poskytnutie informácie.

8.4 V súlade s bodom 8.3 Zmluvy, Tretia strana poskytne Prevádzkovateľovi základnej služby najmä nasledovné informácie:

8.4.1 informácie potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované Prevádzkovateľom základnej služby, Národným bezpečnostným úradom alebo iným orgánom vykonávajúcim pôsobnosť v oblasti kybernetickej bezpečnosti (vrátane jednotiek CSIRT) , alebo orgánmi činnými v trestnom konaní za účelom splnenia povinností Prevádzkovateľa základnej služby v zmysle Zákona alebo príslušnej požiadavky orgánu verejnej moci,

8.4.2 informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní (vrátane dôkazu samotného),

8.4.3 informácie potrebné na účely splnenia povinnosti Prevádzkovateľa základnej služby v zmysle § 19 ods.6 písm. e) Zákona oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

8.4.4 informácie v potrebnom rozsahu na účely splnenia povinnosti Prevádzkovateľa základnej služby v zmysle Zákona, najmä v zmysle § 27, 27a, 27b a 27c Zákona.

Článok 9
Notifikačné povinnosti

9.1 Tretia strana je povinná bez zbytočného odkladu informovať Prevádzkovateľ základnej služby o kybernetickom bezpečnostnom incidente Prevádzkovateľa základnej služby. Informovaním o kybernetickom bezpečnostnom incidente sa rozumie poskytnutie všetkých informácií o kybernetickom bezpečnostnom incidente, o ktorých má alebo by mala mať Tretia strana vedomosť. Pre vylúčenie pochybností platí, že kybernetickým bezpečnostným incidentom sa rozumie udalosť v zmysle § 3 písm. k) Zákona (v znení zákona č. 231/2022 Z. z., príp. v znení neskorších predpisov) a rozsah informácií o kybernetickom bezpečnostnom incidente je daný rozsahom vyžadovaným na splnenie si povinnosti Prevádzkovateľa základnej služby v zmysle § 24 Zákona (v znení zákona č. 231/2022 Z. z.) prostredníctvom jednotného informačného systému kybernetickej bezpečnosti alebo iného komunikačného kanála (vrátane dodatočných dopytov a požiadaviek orgánov vykonávajúcich pôsobnosť v oblasti kybernetickej bezpečnosti alebo jednotiek CSIRT v zmysle Zákona).

9.2 V nadväznosti na bod 9.1 Zmluvy je Tretia strana povinná poskytnúť Prevádzkovateľovi základnej služby najmä nasledovné informácie o kybernetickom bezpečnostnom incidente:

9.2.1 funkcia a pracovné zaradenie osoby Tretej strany, ktorá hlási kybernetický bezpečnostný incident;
9.2.2 identifikačné údaje ďalších osôb dotknutých kybernetickým bezpečnostným incidentom;
9.2.3 informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu, najmä (ak relevantné):

9.2.3.1. kategória kybernetického bezpečnostného incidentu v zmysle Vyhlášky č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov;
9.2.3.2. typ kybernetického bezpečnostného incidentu (napr. pokus o prienik do systému,
9.2.3.3. podozrenie na úspešný prienik do systému vrátane APT, nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby), neoprávnený prístup k informáciám, únik informácií, poškodenie informácií, podvod (neautorizované využitie prostriedkov, porušenia autorských práv), iné,
9.2.3.4. identifikácia nežiaduceho obsahu (napr. spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
9.2.3.5. identifikácia škodlivého kódu (napr. vírus, malvér, ransomvér),
9.2.3.6. spôsob identifikácie kybernetického bezpečnostného incidentu a informácií o kybernetickom bezpečnostnom incidente (skenovanie siete, odpočúvanie, sociálne inžinierstvo),
9.2.3.7. identifikácia zraniteľnosti,

9.2.4 časové údaje zistenia a vzniku kybernetického bezpečnostného incidentu,
9.2.5 čas začiatku incidentu (ak je známy), informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,
9.2.6 detailný opis priebehu kybernetického bezpečnostného incidentu a jeho prvotná príčina,
9.2.7 popis rozsahu a odhad výšky škôd,
9.2.8 odhad závažnosti dopadu kybernetického bezpečnostného incidentu na tretie strany,
9.2.9 identifikácia ohrozenej alebo narušenej základnej služby a ďalšie v dôsledku kybernetického bezpečnostného incidentu, najmä:

9.2.9.1. ohrozené alebo narušené aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby,
9.2.9.2. informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity základnej služby alebo činností Prevádzkovateľa základnej služby a či je aktívum v čase podávania hlásenia v prevádzke,

9.2.10 informácie o riešení kybernetického bezpečnostného incidentu,
9.2.11 stav riešenia kybernetického bezpečnostného incidentu,
9.2.12 informácia o vykonaní opatrení smerujúcich k riešeniu hláseného kybernetického bezpečnostného incidentu,
9.2.13 opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,
9.2.14 výsledok prijatých opatrení,
9.2.15 dátum a čas realizácie opatrení.

9.3 Tretia strana je povinná bez zbytočného odkladu informovať Prevádzkovateľa základnej služby o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti. V prípade pochybností Zmluvné strany berú na vedomie, že vplyv na zabezpečovanie kybernetickej bezpečnosti majú akékoľvek informácie, ktoré svedčia alebo nasvedčujú ohrozenie alebo porušenie požiadaviek

Zákona, Vyhlášky, Zmluvy alebo ohrozenie alebo narušenie kontinuity základnej služby, ktorých včasná znalosť alebo dispozícia s nimi by mala alebo mohla mať akýkoľvek vplyv na kybernetickú bezpečnosť alebo práva alebo právom chránené záujmy Zmluvných alebo tretích osôb.

9.4 Zmluvné strany sú povinné vzájomne sa informovať o všetkých skutočnostiach, ktoré môžu mať akýkoľvek vplyv na Zmluvu, najmä na jej plnenie ktoroukoľvek Zmluvnou stranou.

9.5 Z dôvodu rýchlosti a efektívnosti komunikácie Zmluvných strán, pokiaľ sa Zmluvné strany nedohodnú na širšom rozsahu komunikácie, bude komunikácia Zmluvných strán podľa prebiehať prostredníctvom mailových adries Zmluvných strán uvedených v záhlaví Zmluvy alebo Zmluvnými stranami oznámenými iným preukázateľným spôsobom. Informácia poskytovaná podľa tohto bodu Zmluvy sa považuje za doručenú prvý pracovný deň nasledujúci po dni, v ktorom bola informácia Zmluvnou stranou odoslaná druhej Zmluvnej strane, a to aj vtedy, ak sa o nej druhá Zmluvná strana nedozvedela alebo sa s touto neoboznámila.

Článok 10
Kontrolná činnosť a audit

10.1 Výkonom kontrolných činnosti a auditu sa rozumie požiadavka Prevádzkovateľa základnej služby na výkon kontroly alebo auditu Prevádzkovateľom základnej služby alebo ním poverenej osoby u Tretej strany na overenie plnenia povinností Treťou stranou, ktoré jej vyplývajú zo Zmluvy, a to v rozsahu a za podmienok podľa § 28 a 29 Zákona (v znení zákona č. 231/2022 Z. z.), ak Zmluva neurčuje inak (ďalej ako „**Kontrola**" alebo „**výkon Kontroly**"). Pre vylúčenie pochybností platí, že postup Prevádzkovateľa základnej služby podľa § 29 Zákona je možné zabezpečiť len prostredníctvom certifikovaného audítora kybernetickej bezpečnosti. Zmluvné strany sa dohodli na nasledovnom rozsahu, spôsobe a možnostiach výkonu Kontroly u Tretej strany:

10.1.1 Tretia strana je povinná na požiadanie Prevádzkovateľa základnej služby v primeranom čase nie dlhšom ako 5 dní od doručenia žiadosti Prevádzkovateľa základnej služby umožniť Kontrolu vykonávanú Prevádzkovateľom základnej služby alebo ním poverenou osobou, ktorého Prevádzkovateľ základnej služby výkonom Kontroly poveril;

10.1.2 žiadosť Prevádzkovateľa základnej služby o výkon Kontroly u Tretej strany musí byť Prevádzkovateľom základnej služby predložená v dostatočnom časovom predstihu pred požadovaným výkonom Kontroly, najmenej však 5 dní pred požadovaným výkonom Kontroly a musí obsahovať informácie o termíne, zameraní a mieste výkonu Kontroly a identifikáciu zástupcov Prevádzkovateľa základnej služby, ktorí sa Kontroly zúčastnia;

10.1.3 zástupcovia Prevádzkovateľa základnej služby zúčastňujúci sa Kontroly alebo vykonávajúci Kontrolu sú povinní dodržiavať všetky právne predpisy a interné predpisy Tretej strany, s ktorými boli Treťou stranou oboznámení;

10.1.4 Tretia strana je povinná pri Kontrole 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 Zmluvy alebo Hlavnej zmluvy;

10.1.5 Prevádzkovateľ základnej služby je v rámci Kontroly oprávnený klásť otázky zamestnancom a subdodávateľom Tretej strany, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa Zmluvy za prítomnosti osoby poverenej Treťou stranou.

10.1.6 náklady spojené s výkonom Kontroly znáša Prevádzkovateľ základnej služby.

10.2 Ak Tretia strana neumožní vykonanie Kontroly, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy. Pre takýto prípad je Prevádzkovateľ základnej služby oprávnený od tejto Zmluvy odstúpiť.

10.3 Tretia strana je povinná v lehote určenej Prevádzkovateľom základnej služby, nie však skôr ako v lehote 60 dní odo dňa ich oznámenia, prijať opatrenia na nápravu nedostatkov zistených Kontrolou a poskytnúť Prevádzkovateľovi základnej služby potrebnú súčinnosť.

10.4 Tretia strana je povinná pre prípad zániku Zmluvy Prevádzkovateľovi základnej služby vrátiť alebo previesť všetky informácie, ku ktorým má Tretia strana na základe Zmluvy počas jej trvania prístup alebo tieto informácie zničiť. Tretia strana je pre účely tohto bodu Zmluvy povinná Prevádzkovateľ základnej služby dodatočne preukázať, že postupovala v súlade s týmto bodom Zmluvy, a to prípadne prostredníctvom písomného vyhlásenia Tretej strany o konkrétnom postupe Tretej strany v zmysle tohto bodu Zmluvy.

10.5 Ustanovenia tohto článku Zmluvy sa primerane vzťahujú aj na výkon Kontroly u Subdodávateľa. V zmysle článku Článok 4 Zmluvy je Tretia strana povinná povinnosťou podriadiť sa výkonu Kontroly zaviazať aj všetkých svojich Subdodávateľov.

Článok 11
Rozsah činností Tretej strany

11.1 Zmluvné strany vyhlasujú, že konkrétny rozsah činností Tretej strany je daný Hlavnou zmluvou, pričom pokiaľ sa jedná o činnosti súvisiace s kybernetickou bezpečnosťou, rozsah činností je daný touto Zmluvou v spojení s bodom 2.4 a 2.5 Zmluvy.

Článok 12
Povinnosti po skončení Zmluvy

12.1 Zmluvné strany berú na vedomie, že predmetom plnenia Hlavnej zmluvy môže byť autorské dielo podľa zákona č. 185/2015 Z. z. Autorský zákon v platnom znení, ktorého súčasťou môže byť:

12.1.1 softvér, ktorý bol vytvorený Treťou stranou predovšetkým pre podmienky a potreby Prevádzkovateľa základnej služby;
12.1.2 softvér Tretej strany, ktorý má všeobecný charakter;
12.1.3 softvér tretích osôb; alebo
12.1.4 Open Source softvér, ktorý je podriadený príslušnej licencii slobodného softvéru.

12.2 Zmluvné strany berú ďalej na vedomie, že predmetom plnenia Hlavnej zmluvy 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 Tretej strany.

12.3 S ohľadom na body 12.1 a 12.2 Zmluvy Tretia strana vyhlasuje, že v zmysle § 9 ods. 2 písm. p) Vyhlášky umožní Prevádzkovateľovi základnej služby zabezpečiť kontinuitu prevádzkovanej základnej služby vo vzťahu k Plneniu a na tieto účely je povinná udeliť, poskytnúť, previesť alebo postúpiť Prevádzkovateľovi základnej služby všetky potrebné licencie, práva alebo súhlasy na zabezpečenie kontinuity prevádzkovanej základnej služby.

12.4 Zmluvné strany sa dohodli, že spôsob splnenia povinnosti Tretej strany podľa bodu 12.3 Zmluvy je na uvážení Prevádzkovateľa základnej služby v rozsahu nevyhnutnom na naplnenie podmienky v zmysle § 8 ods. 2 písm. p) Vyhlášky.

Článok 13
Zodpovednosť za škodu a sankcie

13.1 Zmluvná strana zodpovedá za škodu spôsobenú druhej Zmluvnej strane. Za škodu vzniknutú Zmluvnej strane sa na účely Zmluvy považuje aj pokuta alebo akákoľvek iná sankcia uložená Zmluvnej strane príslušným štátnym orgánom. V prípade, že Zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo Zákona alebo Zmluvy (ďalej ako „**porušujúca Zmluvná strana**") a v dôsledku tohto konania alebo opomenutia konania porušujúcej zmluvnej strany dôjde k vzniku škody na strane druhej Zmluvnej strany (ďalej ako „**poškodená Zmluvná strana**"), postupujú Zmluvné strany v zmysle platnej legislatívy.

Článok 14
Doručovanie

14.1 Ak Zmluvou nie je uvedené inak, písomnosti si doručujú Zmluvné strany na:

14.1.1 adresu uvedenú v záhlaví Zmluvy, ibaže Zmluvná strana oznámi písomne druhej Zmluvnej strane zmenu adresy;
14.1.2 mailovú adresu uvedenú v záhlaví Zmluvy alebo Zmluvnou stranou oznámenú spôsobom podľa bodu 14.1.1 Zmluvy

14.2 Písomnosť podľa bodu 14.1.1 Zmluvy sa považuje za doručenú, ak:

14.2.1 sa druhá Zmluvná strana o písomnosti nedozvedela, a to piatym dňom odo dňa jej preukázateľného odoslania na adresu druhej Zmluvnej strany doporučenou poštou alebo kuriérom;
14.2.2 dňom prevzatia písomnosti alebo dňom odmietnutia prevziať písomnosť pri osobnom doručovaní.

14.3 Písomnosť podľa bodu 14.1.2 Zmluvy sa považuje za doručenú v zmysle podmienok podľa bodu 9.5 Zmluvy.

Článok 15
Záverečné ustanovenia

15.1 Zmluva je vyhotovená v dvoch vyhotoveniach. Každá Zmluvná strana dostane po jednom vyhotovení. Neoddeliteľnou súčasťou Zmluvy sú nasledovné Prílohy:

15.1.1 *Príloha č. 1*: Analýza rizík;
15.1.2 *Príloha č. 2*: Bezpečnostné politiky Prevádzkovateľa základnej služby;
15.1.3 *Príloha č. 3*: Zoznam pracovných rolí Tretej strany a ich personálne obsadenie;
15.1.4 *Príloha č. 4*: Špecifikácia a rozsah bezpečnostných opatrení.

15.2 Pokiaľ nie je v Zmluve uvedené inak, riadia sa práva a povinnosti Zmluvných strán Zákonom a Obchodným zákonníkom.

15.3 Zmluvu je možné meniť, upravovať alebo dopĺňať iba písomnými dodatkami, ktoré sa po podpísaní obidvoma Zmluvnými stranami stávajú jej neoddeliteľnou súčasťou.

15.4 Sporné otázky vyplývajúce zo Zmluvy sa budú prednostne riešiť dohodou Zmluvných strán a až potom, keď sa ich nepodarí vyriešiť dohodou, prostredníctvom súdu. Zmluvné strany si dohodli lehotu 60 dní na vyriešenie sporných otázok dohodou Zmluvných strán. Lehotu podľa predchádzajúcej vety je možné Zmluvnými stranami predĺžiť o ďalších 60 dní, a to aj opakovane. Predĺžením lehoty sa rozumie aj konkludentný prejav vôle Zmluvnej strany spočívajúci v účasti na rokovaniach alebo riešení sporných otázok inou cestou aj po uplynutí lehoty podľa tohto bodu Zmluvy.

15.5 V prípade, že je alebo sa stane niektoré ustanovenie Zmluvy neplatné, zostávajú ostatné ustanovenia Zmluvy platné a účinné. Namiesto neplatného ustanovenia sa použijú ustanovenia všeobecne záväzných právnych predpisov upravujúce otázku vzájomného vzťahu Zmluvných strán. Zmluvné strany sa potom zaväzujú upraviť svoj vzťah prijatím iného ustanovenia, ktoré svojím obsahom a povahou najlepšie zodpovedá zámeru neplatného ustanovenia.

Zmluvné strany prehlasujú, že ustanoveniam Zmluvy porozumeli čo do obsahu i rozsahu, Zmluva vyjadruje ich slobodnú vôľu, na znak čoho k nej pripájajú svoje podpisy.

V Galante dňa	V Nových Zámkoch dňa .....
Za Prevádzkovateľa základnej služby:	Za Tretiu stranu:
Mesto Galanta Mgr. Peter Kolek primátor	NOVITECH Nové Zámky, s.r.o. Ing. Štefan Horváth konateľ

Príloha č. 1

K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Výstup z Analýzy rizík

1. Tretia strana poskytne PZS, na základe požiadaviek PZS, IT služby súvisiace so zriadením virtuálnej platformy v prostredí **Microsoft AZURE** (ďalej len MSA) nevyhnutnej pre výkon činností PZS. Na vytvorenej virtuálnej platforme bude následne PZS využívať cloudové služby poskytované spoločnosťou Microsoft.

2. Poskytovateľom cloudových služieb platformy MSA pre PZS je **spoločnosť Microsoft**. Tretia strana PZS cloudové služby v platforme MSA neposkytuje. Tretia strana len na základe požiadaviek PZS cloudové služby v MSA pre PZS spúšťa, konfiguruje, ruší, nastavuje, vypína a kontroluje ich.

3. Tretia strana po zriadení cloudových služieb pre PZS v prostredí MSA odovzdá PZS prihlasovacie údaje pre prístup do prostredia MSA, pre PZS vytvoreným cloudovým službám a prostriedkom. PZS môže bezprostredne tieto údaje zmeniť, čím zamedzí aj prístup tretej strane. Bude v plnej kompetencii PZS a jeho zodpovednosti, komu prihlasovacie údaje poskytne.

4. Cloudová platforma Microsoft Azure (MSA) nezabezpečuje, že aplikácie prevádzkované PZS na platforme MSA budú v súlade s NIS2, resp. so zákonom o kybernetickej bezpečnosti. Ide o zdieľanú zodpovednosť, kde spoločnosť Microsoft je zodpovedná za svoju cloudovú platformu AZURE, PZS je zodpovedný za svoje aplikácie prevádzkované na MSA platforme. MSA platforma poskytuje len nástroje (logovanie, monitoring, politiky,...), ktoré PZS umožňujú svoje aplikácie nakonfigurovať a prevádzkovať tak, že budú v súlade s NIS2, resp. so zákonom o kybernetickej bezpečnosti.

5. Spoločnosť Microsoft zverejňuje informácie o compliance štandardoch ktoré platforma MSA spĺňuje na nasledovnej adrese: https://learn.microsoft.com/en-us/azure/compliance/

6. Tretia strana nebude mať prístup k obsahu, k dátam, ktoré si PZS presunie a bude prevádzkovať na platforme MSA. Tretia strana nie je zodpovedná za bezpečnosť, vecnú ani obsahovú stránku dát patriacich PZS vo virtuálnom prostredí MSA, prevádzkovanej spoločnosťou Microsoft.

7. Tretia strana nebude mať prístup do lokálnej počítačovej siete PZS.

8. Riziká
   - 8.1 Tretej strane nie sú známe **žiadne zásadné riziká** pre PZS spojené s využívaním cloudového systému Microsoft AZURE.
   - 8.2 Existuje riziko poruchy-nefunkčnosti niektorej zo služieb cloudového systému MSA, ale na základe dlhoročných skúseností tretej strany s MSA je toto riziko mimoriadne nízke. V drvivej väčšine tretej strane hlásených porúch PZS išlo o poruchy spôsobené poruchou na pripojení PZS k internetu, preto tretia strana doporučuje prevádzkovať záložné pripojenie k internetu. Ak sa vyskytne porucha na akejkoľvek službe MSA, je ju možné odstrániť vo veľmi krátkom čase. Spoločnosť Microsoft garantuje najvyššiu mieru dostupnosti prostriedkov MSA zo všetkých aktuálnych poskytovateľov cloudových služieb.
   - 8.3 Tretia strana nenesie zodpovednosť za možné riziká, ktoré vyplývajú z prevádzkovania informačného systému ani akéhokoľvek iného softvéru PZS v prostredí MSA, o ktorých nemohla vopred vedieť, ako sú napríklad prípadné kybernetické útoky. Je povinnosťou PZS dostatočne si zabezpečiť dáta v prostredí MSA.
   - 8.4 PZS využívaním služieb MSA eliminuje riziko fyzického útoku na IT infraštruktúru prevádzkovanú v MSA, zároveň eliminuje riziko straty dát, ktoré budú v tomto prostredí aj zálohované.

Príloha č. 2

K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Bezpečnostné politiky Prevádzkovateľa základnej služby a smernice:

- Bezpečnostný projekt.
- Informačné systémy verejnej správy a kybernetická bezpečnosť.
- Organizačná smernica – fyzická bezpečnosť a bezpečnosť prostredia.
- Smernica pre používanie aktív so zreteľom na ochranu osobných údajov pre správcov informačného systému.
- Smernica pre riešenie bezpečnostných incidentov v oblasti ochrany osobných údajov.

Príloha č. 3

K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Zoznam pracovných rolí Tretej strany a ich personálne obsadenie:

1) Meno a priezvisko: Ing. Norbert Viola
   Pracovná rola: špecialista pre cloudové služby Microsoft AZURE

2) Meno a priezvisko: Ing. Štefan Horváth
   Pracovná rola: manažér, administratíva

Tento zoznam zahŕňa aj budúci zoznam personálneho obsadenia Tretej strany v prípade zmeny a doplnenia zamestnancov a partnerov.

Príloha č. 4

K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Špecifikácia a rozsah všeobecných bezpečnostných opatrení

1.1 Oblasť riadenia prístupov sa zabezpečuje nasledovne:

1.1.1 vypracovania zásad riadenia prístupu k informáciám;
1.1.2 riadenia prístupu používateľov;
1.1.3 vymedzenie príslušných zodpovedností používateľov;
1.1.4 riadenia prístupu k sieťam, čím sa rozumie:

1.1.4.1. že každému používateľovi siete a informačného systému sa prideľuje jednoznačný identifikátor na autentizáciu na vstup do siete a informačného systému;
1.1.4.2. zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov;
1.1.4.3. využívanie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroja na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy);
1.1.4.4. výkon kontroly prístupových účtov a prístupových oprávnení v pravidelných intervaloch, najmenej však raz za 6 mesiacov na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov;
1.1.4.5. určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle bezpečnostnej stratégie alebo príslušnej bezpečnostnej politiky Prevádzkovateľa základnej služby;

1.1.5 riadenie prístupu k operačnému systému a jeho službám;
1.1.6 riadenie prístupu k aplikáciám;
1.1.7 monitorovanie prístupu a používania informačného systému; a
1.1.8 riadenie vzdialeného prístupu.

1.1.9 Riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.

1.1.10 Riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb Prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.

1.2 Oblasť hodnotenia zraniteľností a bezpečnostných aktualizácií sa zabezpečuje nasledovne:

1.2.1 Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom

1.2.1.1. nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
1.2.1.2. nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
1.2.1.3. využitia verejných zoznamov a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

1.2.2 Cieľom procesu riadenia záplat a aktualizácií je zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií a plošnú aplikáciu aktualizácií na zariadenia, pre ktoré je softvérová aktualizácia či záplata vydaná.

1.2.3 Úlohami procesu riadenia záplat a aktualizácií sú najmä

1.2.3.1. identifikácia potrieb softvérových záplat a aktualizácií,
1.2.3.2. evidencia softvérových záplat a aktualizácií a informácia o ich nasadení alebo o dôvodoch ich nenasadenia,
1.2.3.3. rozhodnutie o vhodnom prístupe k otestovaniu softvérových záplat a aktualizácií,
1.2.3.4. zabezpečenie implementácie softvérových záplat a aktualizácií,
1.2.3.5. aktualizácia plánu softvérových záplat a aktualizácií.

1.2.4 Neschválené aktualizácie nie sú prípustné.

1.3 Oblasť ochrany proti škodlivému kódu sa zabezpečuje nasledovne:

1.3.1 Požiadavkami na ochranu proti škodlivému kódu sú najmä

1.3.1.1. určenie zodpovednosti používateľov za prevenciu pred škodlivým kódom,
1.3.1.2. určenie pravidiel pre inštaláciu a používanie systémov prevencie škodlivého kódu,
1.3.1.3. monitorovanie potenciálnych ciest prieniku škodlivého kódu do prostredia sietí a informačných systémov.

1.3.2 Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že

1.3.2.1. v reálnom čase vykonávajú kontrolu prístupu k digitálnemu obsahu vrátane sieťovej prevádzky, sťahovania, spúšťania alebo otvárania súborov, priečinkov na vymeniteľnom alebo vzdialenom úložisku a prístupu k webovým sídlam a cloudovým službám,
1.3.2.2. spúšťajú pravidelné kontroly úložísk vrátane cloudových a pripojených vymeniteľných úložísk, najmenej raz ročne,
1.3.2.3. neoprávneným používateľom je zabránené v prístupe k obsahu prostredníctvom funkcie filtrovania obsahu,
1.3.2.4. používateľom je zamedzené v pokusoch odinštalovať alebo zakázať funkcie systému na ochranu proti škodlivému kódu.

1.4 Oblasť sieťovej a komunikačnej bezpečnosti sa zabezpečuje nasledovne:

1.4.1 Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä

1.4.1.1. prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami, a to najmä využitím nástrojov na ochranu integrity sietí, ktoré sú zabezpečené segmentáciou sietí, informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len informačné systémy s rovnakými bezpečnostnými požiadavkami, rovnakej kategórie a s podobným účelom,

1.4.1.2. tým, že spojenia medzi segmentmi siete, ktoré sú chránené firewallom sú povoľované na princípe zásady najnižších privilégií,

1.4.1.3. prostredníctvom bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup, napríklad s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,

1.4.1.4. tým, že v sieťach sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete,

1.4.1.5. tým, že spojenia do externých sietí sú smerované cez sieťový firewall,

1.4.1.6. prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,

1.4.1.7. udržiavaním zoznamu vstupno-výstupných bodov na hranici siete v aktuálnom stave,

1.4.1.8. použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,

1.4.1.9. prostredníctvom blokovania neoprávnených spojení zo zdrojov identifikovaných ako škodlivé alebo spôsobujúce hrozby, ak to nastavenie informačného systému umožňuje,

1.4.1.10. neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty,

1.4.1.11. prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,

1.4.1.12. v závislosti od prostredia implementovaním systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,

1.4.1.13. prostredníctvom smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,

1.4.1.14. prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,

1.4.1.15. vykonávaním pravidelného alebo nepretržitého posudzovania technických zraniteľností, a posudzovania technických zraniteľností zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

1.5 Oblasť zaznamenávania udalostí a monitorovania sa zabezpečuje nasledovne:

1.5.1 Zaznamenávanie udalostí a monitorovanie sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu

1.5.1.1. centrálnych sieťových prvkov a serverov,

1.5.1.2. služieb prístupných do externých sietí a

1.5.1.3. kritických interných serverov a služieb.

1.5.2 Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej

1.5.2.1. aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených,
1.5.2.2. iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,
1.5.2.3. pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla,
1.5.2.4. automatické varovné alebo chybové hlásenia systémov,
1.5.2.5. detegované podozrivé alebo škodlivé aktivity a
1.5.2.6. ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.

1.5.3 Prevádzkové záznamy sú zabezpečené najmenej tak, že

1.5.3.1. sú čitateľné výlučne osobám povereným ich analýzou,
1.5.3.2. zamedzujú možnosti prepísania alebo vymazania záznamu,
1.5.3.3. záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete,
1.5.3.4. sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

1.5.4 Za monitorovanie prevádzkových záznamov, ich vyhodnocovanie a vykonanie nahlásenia podozrivej aktivity je zodpovedný na to poverený zamestnanec prevádzkovateľa základnej služby alebo zamestnanec tretej strany, ak je jej táto činnosť zverená.

1.6 Oblasť riešenia kybernetických bezpečnostných incidentov sa zabezpečuje nasledovne:

1.6.1 Riešenie kybernetických bezpečnostných incidentov pozostáva najmä

1.6.1.1. z prípravy a vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov,
1.6.1.2. z monitorovania a analyzovania udalostí v sieťach a informačných systémoch,
1.6.1.3. z detekcie kybernetických bezpečnostných incidentov,
1.6.1.4. zo zberu relevantných informácií o kybernetických bezpečnostných incidentoch,
1.6.1.5. z vyhodnocovania kybernetických bezpečnostných incidentov,
1.6.1.6. z riešenia zistených kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov a
1.6.1.7. z vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatia opatrení alebo zavedenia nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov.

1.6.2 Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmä

1.6.2.1. postup pri internom nahlasovaní kybernetických bezpečnostných incidentov,
1.6.2.2. postup pri hlásení kybernetických bezpečnostných incidentov podľa § 24 ods. 1 zákona,
1.6.2.3. postup pri riešení jednotlivých typov kybernetických bezpečnostných incidentov a spôsob ich vyhodnocovania a
1.6.2.4. spôsob evidencie kybernetických bezpečnostných incidentov a použitých riešení.

1.6.3 Proces detekcie kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.

1.6.4 Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje

1.6.4.1. zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch,
1.6.4.2. vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom,
1.6.4.3. vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov,
1.6.4.4. revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.

1.6.5 Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom

1.6.5.1. pridelenia zodpovednosti a určenia postupov na zvládanie kybernetických bezpečnostných incidentov,
1.6.5.2. zavedenia procesu získavania a uchovávania podkladov potrebných na analýzu kybernetickej bezpečnostnej udalosti a kybernetického bezpečnostného incidentu,
1.6.5.3. prijímania opatrení na odvrátenie alebo zmiernenie vplyvu kybernetického bezpečnostného incidentu,
1.6.5.4. zavedenia pravidelného testovania, najmenej raz ročne, procesu nahlasovania kybernetických bezpečnostných incidentov, v zmysle štandardov a postupov vypracovaných podľa odseku 2, s vedením záznamov o takomto testovaní,
1.6.5.5. vedenia záznamov o kybernetických bezpečnostných incidentoch vrátane použitých riešení,
1.6.5.6. prešetrovania a určenia príčin vzniku kybernetického bezpečnostného incidentu,
1.6.5.7. aktualizácie bezpečnostnej politiky a prijatia primeraných bezpečnostných opatrení zamedzujúcich opakovanému výskytu kybernetického bezpečnostného incidentu a
1.6.5.8. určenia fyzickej osoby zodpovednej za nahlasovanie a odovzdávanie hlásení o kybernetických bezpečnostných incidentoch.

1.6.6 Súčasťou evidencie kybernetických bezpečnostných incidentov sú na zabezpečenie dôkazu alebo dôkazného prostriedku aj informácie, na základe ktorých sa identifikuje vznik a pôvod kybernetického bezpečnostného incidentu.

Špecifikácia a rozsah bezpečnostných opatrení vyplývajúcich z analýzy rizík

1. Keďže z pohľadu vzťahu PZS a tretej strany sa za jediné riziko považuje nefunkčnosť cloudového systému MSA, nie sú potrebné žiadne bezpečnostné opatrenia. Spoločnosť Microsoft garantuje 99,9%-nú dostupnosť služieb AZURE.
2. Na všeobecné riziko kybernetických útokov budú využívané bezpečnostné opatrenia zo strany PZS a bezpečnostné opatrenia a zároveň zo strany spoločnosti Microsoft, ktorá cloudové služby pre PZS poskytuje.
3. Spoločnosť Microsoft garantuje vysokú bezpečnosť dát umiestnených v prostredí AZURE.
   V MSA budú dáta PZS chranené voči ich zničeniu (živelná pohroma, požiar, ...), Microsoft chráni dáta ich viacnásobnou kópiou v Locally redundant riešení, spolu s dalšími kópiami dát v inej lokácii (Geo redundant).