

177/2020

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. O-20/0048

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

Tretia strana	GAMO a.s. Kyjevské námestie 6 974 04 Banská Bystrica
Banka	Slovenská sporiteľňa, a. s., pobočka Banská Bystrica č. ú. 0435467048/0900 IBAN: SK5409000000000435467048 BIC: GIBASKBX Majiteľ účtu: GAMO a.s. Kyjevské námestie 6 974 04 Banská Bystrica
Obchodný register	Okresný súd Banská Bystrica oddiel Sa, vl. č. 550/S
IČO	36033987
DIČ	2020087498
IČ DPH	SK2020087498
Štatutárny zástupca	Ing. Kristián Alakša – predseda predstavenstva Iveta Milčíková – podpredseda predstavenstva Ing. Rudolf Latiak – člen predstavenstva

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

a

Prevádzkovateľ základnej služby	Trnavská vodárenská spoločnosť, a.s. Priemyselná 10 Piešťany
Banka	Bank. spojenie : VÚB, a.s. Číslo účtu IBAN: SK71 0200 0000 2700 0300 2212
Obchodný register	Zapísaný v Obchodnom registri Okresného súdu Trnava, oddiel Sa, Vložka číslo:10263/T
IČO	36 252 484
DIČ	32020172264
IČ DPH	SK2020172264
Štatutárny zástupca	Ing. Vladimír Púčik - predseda predstavenstva Ivan Šiška - podpredseda predstavenstva
Zástupca oprávnený rokovať vo veciach technických	kontaktná osoba: Ing. Miroslav Sedlák e-mail: sedlak@tavos.sk

	tel. č.: +421 33 59 66 187
--	----------------------------

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

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

PREAMBULA

NAKOLKO Prevádzkovateľ základnej služby s ohľadom na predchádzajúci odsek s treťou stranou uzatvoril Zmluvu o poskytovaní servisných služieb SLA Cisco produktov pre LAN a WAN (ďalej ako „**Zmluva o službách**“), ktorá určuje obsah a rozsah služieb poskytovaných treťou stranou Prevádzkovateľovi základnej služby, ktorými sú služby zabezpečenia servisu Cisco produktov pre LAN a WAN pre Prevádzkovateľa základnej služby v rozsahu podľa Zmluvy o službách (ďalej ako „**Služby**“);

NAKOLKO Prevádzkovateľ základnej služby vyhlasuje, že Služby poskytované treťou stranou priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa základnej služby, v dôsledku čoho je povinný v zmysle § 19 ods. 2 Zákona uzatvoriť s treťou stranou zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti Zmluvy o službách;

NAKOLKO Prevádzkovateľ základnej služby vyhlasuje, že pred uzatvorením tejto zmluvy bola vykonaná analýza rizík podľa bodu 1.2 tejto zmluvy vo vzťahu k dodávaným Službám 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 všeobecne záväzný právny predpis, Zmluva alebo Zmluva o službách. 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 všeobecne záväzný právny predpis;
- 1.1.4 Zmluva; a
- 1.1.5 Zmluva o službách.

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 § 8 ods. 1 Vyhlášky pri uzatvorení zmluvy s Treťou stranou podľa § 19 ods. 2 Zákona, a teda pri uzatvorení Zmluvy boli analyzované riziká spojené s dodávaním Služieb Treťou stranou spôsobom podľa § 6 Vyhlášky (ďalej ako „**Analýza rizík**“). Analýza rizík 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 riziko a jeho kvantifikácia; a
- 1.2.5 vlastník rizika.



- 1.3 Prevádzkovateľ základnej služby súčasne vyhlasuje, že v rámci Analýzy rizík neidentifikoval také riziká, ktoré by odôvodňovali prípadné neuzatvorenie Zmluvy s Tretou stranou alebo zánik Zmluvy o službách.
- 1.4 Tretia strana vyhlasuje a súhlasí, že bude dodržiavať všetky bezpečnostné politiky Prevádzkovateľa základnej služby v rozsahu, v akom ho s nimi Prevádzkovateľ základnej služby preukázateľne oboznámil. Uvedené sa týka aj akejkoľvek úpravy, zmeny alebo doplnenia bezpečnostných politík Prevádzkovateľa základnej služby počas platnosti Zmluvy. Bezpečnostné politiky Prevádzkovateľa základnej služby aktuálne ku dňu podpisu Zmluvy tvoria Prílohu č. 2 Zmluvy.
- 1.5 V prípade, ak sa ktorékoľvek vyhlásenie podľa ustanovenia Článok 1 Zmluvy ukáže ako nepravdivé, Zmluvná strana, ktorá takéto nepravdivé vyhlásenie poskytla, zodpovedá za škodu druhej Zmluvnej strane alebo tretej osobe, ktorá Zmluvnej strane alebo tretej osobe v tejto súvislosti vznikla, a to v celom rozsahu.

Článok 2

Predmet Zmluvy

- 2.1 Predmetom Zmluvy je úprava práv a povinností Zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa základnej služby.
- 2.2 Pre účely Zmluvy sa činnosťami, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa základnej služby rozumejú Služby Tretej strany podľa Zmluvy o službách.
- 2.3 Zmluvné strany sa dohodli, že Prevádzkovateľ základnej služby a Tretia strana si poskytnú všetku primeranú súčinnosť pri plnení Zmluvy.
- 2.4 Pre vylúčenie akýchkoľvek pochybností platí, že Tretia strana nemá žiadne povinnosti podľa Zmluvy a nie je povinná poskytnúť súčinnosť Prevádzkovateľovi základnej služby pri plnení tých bezpečnostných opatrení a notifikačných povinností, ktoré nie sú predmetom Zmluvy a nesúvisia so Zmluvou o službách, aj keď sa jedná o povinnosti Prevádzkovateľa základnej služby vyplývajúce mu zo Zákona.
- 2.5 Zmluvné strany berú na vedomie, že vyčerpávajúci obsah a rozsah povinností Tretej strany vo vzťahu k zabezpečeniu plnenia bezpečnostných opatrení a notifikačných povinností podľa Zmluvy je uvedený v ustanoveniach čl. 8 a čl. 9 Zmluvy.

Článok 3

Subdodávateľ Tretej strany

- 3.1 [Subdodávateľ] Prevádzkovateľ základnej služby a Tretia strana sa dohodli, že Tretia strana je oprávnená podľa vlastného uváženia a na vlastnú zodpovednosť zapojiť ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho alebo akýmkoľvek spôsobom sa podieľajúceho na Službách pre Prevádzkovateľa základnej služby namiesto Tretej strany alebo spolu s Tretou stranou (ďalej ako „Subdodávateľ“).
- 3.2 Tretia strana je povinná uložiť každému Subdodávateľovi tie povinnosti Tretej strany vyplývajúce zo Zmluvy, ktoré sú primerané s ohľadom na rozsah zapojenia Subdodávateľa do Služieb pre Prevádzkovateľa základnej služby namiesto Tretej strany alebo spolu s Tretou stranou.

Článok 4

Zoznam pracovných rolí

- 4.1 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, tvorí Prílohu č. 3 Zmluvy. Informácie a údaje podľa tohto bodu Zmluvy majú rovnaký význam ako im priznáva Vyhláška.
- 4.2 Na prípadné zmeny Prílohy č. 3 Zmluvy Tretou stranou sa primerane vzťahuje bod 13.1 Zmluvy upravujúci postup pri zmene adresy Zmluvnej strany so spôsobom oznámenia tejto zmeny podľa bodu

8.4 Zmluva. Povinnosť mlčanlivosti podľa Zmluvy sa vzťahuje aj na osoby zastávajúce pracovné roly u Tretej strany podľa tohto bodu Zmluvy.

Článok 5

Platnosť Zmluvy a spôsob jej ukončenia

- 5.1 Zmluva sa uzatvára sa na dobu platnosti Zmluvy o službách. Zmluva nadobúda platnosť dňom podpisu Zmluvy oboma Zmluvnými stranami alebo poslednou z nich a účinnosť v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník.
- 5.2 Zmluvné strany sa dohodli, že k zániku Zmluvy môže dôjsť niektorým z nasledovných spôsobov:
- 5.2.1 dohodou Zmluvných strán;
 - 5.2.2 odstúpením od Zmluvy;
 - 5.2.3 zánikom Zmluvy o službách.
 - 5.2.4 uplynutím doby, na ktorú bola zmluva dohodnutá.
- 5.3 [Odstúpenie] 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 30 dní po doručení písomnej výzvy na odstránenie závadného stavu, ktorá bude špecifikovať toto porušenie. 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.
- 5.4 [Neposkytnutie súčinnosti] Zmluvné strany berú na vedomie, že neposkytnutie súčinnosti Zmluvnou stranou nemá za následok omeškanie druhej Zmluvnej strany.
- 5.5 [Závislé zmluvy] Zmluvné strany sa dohodli, že vzájomný vzťah Zmluvy a Zmluvy o službách sa riadi § 275 ods. 2 a 3 Obchodného zákonníka 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 Zmluve o službách. Vznik a existencia Zmluvy o službách je podmienkou vzniku a existencie Zmluvy. Zánik Zmluvy o službách spôsobuje aj zánik Zmluvy, a to s obdobnými právnymi účinkami, ak Zmluva neustanovuje inak. Zánik Zmluvy nespôsobuje zánik Zmluvy o službách, ak Zmluva neustanovuje inak.
- 5.6 Vzhľadom na obsah Zmluvy je aplikácia akýchkoľvek ustanovení týkajúcich sa kybernetickej bezpečnosti podľa Zákona alebo akejkoľvek povinností Zmluvnej strany v zmysle Zákona obsiahnutých v Zmluve o službách vylúčená, pričom sa vždy uplatnia ustanovenia Zmluvy, ak Zmluva neustanovuje inak. Zmluvné strany svojim podpisom prehlasujú, že uvedená forma zmeny Zmluvy o službách podľa predchádzajúcej vety je dostačujúca a spĺňa všetky požiadavky vyžadované na platnú zmenu obsahu Zmluvy o službách. V prípade akýchkoľvek pochybností o aplikácii ustanovení Zmluvy o službách 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 Zmluvy o službách.

Článok 6

Bezpečnostné opatrenia

- 6.1 Zoznam oblastí, pre ktoré sa bezpečnostné opatrenia prijímajú a dodržiavajú:
 - 6.1.1 technických zraniteľností systémov a zariadení;
 - 6.1.2 riadenia bezpečnosti sietí a informačných systémov;
 - 6.1.3 riadenia prístupov;
 - 6.1.4 riešenia kybernetických bezpečnostných incidentov;
 - 6.1.5 monitorovania, testovania bezpečnosti a bezpečnostných auditov.
- 6.2 Jednotlivé bezpečnostné opatrenia pre oblasti podľa bodu 6.1 Zmluvy tvoria Prílohu č. 4 Zmluvy.
- 6.3 Tretia strana ako vlastník rizík podľa Analýzy rizík vyhlasuje, že prijala bezpečnostné opatrenia pre tieto riziká. Konkrétna špecifikácia a rozsah bezpečnostných opatrení Tretej strany tvorí Prílohu č. 5 Zmluvy.
- 6.4 Tretia strana vyhlasuje, že počas účinnosti Zmluvy bude dodržiavať všetky bezpečnostné opatrenia podľa Prílohy č. 5 Zmluvy.

Článok 7

Povinnosti Zmluvných strán

- 7.1 Prevádzkovateľ základnej služby je povinný Zmluvu, Zmluvu o službách, ako aj akúkoľvek ďalšiu zmluvnú alebo súvisiacu dokumentáciu uzatvorenú s Treťou stranou evidovať v rámci bezpečnostnej dokumentácie spôsobom podľa § 2 ods. 1 písm. c) Vyhlášky.
- 7.2 Tretia strana je povinná chrániť všetky informácie, ktoré jej boli poskytnuté Prevádzkovateľom základnej služby pri plnení Zmluvy. Na tento účel je Tretia strana povinná dodržiavať mlčanlivosť a touto mlčanlivosťou zaviazat 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. Zmluvné strany berú na vedomie, 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. 6 Zmluvy.
- 7.3 Prevádzkovateľ základnej služby je oprávnený požadovať od Tretej strany informácie nevyhnutné na splnenie ktorejkoľvek povinnosti Prevádzkovateľa základnej služby vyplývajúcej zo Zákona v rozsahu Zmluvy. Tretia strana je povinná bez zbytočného odkladu poskytnúť Prevádzkovateľovi základnej služby všetky informácie, ktoré má k dispozícii. Informácie podľa tohto bodu Zmluvy poskytuje Tretia strana bezodkladne po doručení žiadosti Prevádzkovateľa základnej služby o poskytnutie informácie. Prevádzkovateľ základnej služby však nie je oprávnený požadovať od Tretej strany informácie, ktoré vie získať z vlastných zdrojov, vlastnými silami alebo prostriedkami alebo ktoré by mu z iného preukázateľného dôvodu mali byť známe.

Článok 8

Notifikačné povinnosti

- 8.1 Tretia strana je povinná bez zbytočného odkladu informovať o kybernetickom bezpečnostnom incidente Prevádzkovateľa základnej služby. Informovaním o kybernetickom bezpečnostnom incidente sa rozumie poskytnutie všetkých informácií o kybernetickom bezpečnostnom incidente, o ktorých má Tretia strana vedomosť.
- 8.2 Tretia strana je povinná bez zbytočného odkladu informovať Prevádzkovateľa základnej služby o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti, o ktorých sa dozvedela. Týmto ustanovením nie je dotknutá povinnosť Prevádzkovateľa základnej služby sledovať a získavať informácie o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti vlastnou činnosťou alebo z iných zdrojov.

- 8.3 Zmluvné strany sú povinné vzájomne sa informovať o všetkých skutočnostiach, ktoré môžu mať akýkoľvek vplyv na Zmluvu, najmä na jej plnenie ktoroukoľvek Zmluvnou stranou.
- 8.4 [Osobitné formy komunikácie Zmluvných strán] Z dôvodu rýchlosti a efektívnosti komunikácie Zmluvných strán, pokiaľ sa Zmluvné strany nedohodnú na širšom rozsahu komunikácie, bude komunikácia Zmluvných strán podľa bodu 7.3, 8.1 a 8.2 Zmluvy 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 doručení deň nasledujúci po dni, v ktorom bola informácia Zmluvnou stranou odoslaná druhej Zmluvnej strane, a to aj napriek tomu, že sa o nej druhá Zmluvná strana nedozvedela alebo sa s touto neoboznámila.

Článok 9

Kontrolná činnosť a audit

- 9.1 Výkonom kontrolných činností a auditu sa rozumie na požiadanie Prevádzkovateľa základnej služby výkon kontroly Prevádzkovateľom základnej služby alebo ním poverenej osoby u Tretej strany na overenie plnenia povinností Treťou stranou, ktoré jej zo Zmluvy vyplývajú, a to v rozsahu a za podmienok podľa § 28 Zákona, ak Zmluva neurčuje inak (ďalej ako „**Kontrola**“ alebo „**výkon Kontroly**“). Zmluvné strany sa dohodli na nasledovnom rozsahu, spôsobe a možnostiach výkonu Kontroly u Tretej strany:
- 9.1.1 Tretia strana je povinná na požiadanie Prevádzkovateľa základnej služby v primeranom čase umožniť Kontrolu vykonávanú Prevádzkovateľom základnej služby alebo ním poverenou osobou, ktorou môže byť len iný audítor kybernetickej bezpečnosti, ktorého Prevádzkovateľ základnej služby preukázateľne výkonom Kontroly poveril;
- 9.1.2 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, dôvodoch, zameraní a mieste výkonu Kontroly a identifikáciu zástupcov Prevádzkovateľa základnej služby, ktorí sa Kontroly zúčastnia;
- 9.1.3 zástupcovia Prevádzkovateľa základnej služby zúčastňujúci sa Kontroly alebo vykonávajúci Kontrolu sú povinní dodržiavať všetky právne predpisy a interné predpisy Tretej strany a musia Tretej strane pred výkonom Kontroly preukázať svoju odbornú spôsobilosť na výkon Kontroly zameranej na plnenie povinností Tretej strany vyplývajúcich zo Zmluvy (napr. certifikáciu ISO 27001);
- 9.1.4 náklady spojené s výkonom Kontroly u Tretej strany v celom rozsahu znáša tá Zmluvná strana, na ktorej žiadosť sa Kontrola uskutočnila.
- 9.2 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. Prevádzkovateľ základnej služby je povinný bezodplatne a bez zbytočného odkladu poskytnúť súčinnosť Tretej strane pri plnení jej povinností podľa tohto bodu Zmluvy.
- 9.3 Tretia strana však na zničenie informácií podľa bodu 9.2 Zmluvy nie je povinná, pokiaľ osobitný predpis ustanovuje uchovanie týchto informácií alebo ak je uchovanie týchto informácií v záujme Prevádzkovateľa základnej služby alebo slúži na ochranu záujmov Tretej strany.

Článok 10

Rozsah činností Tretej strany

- 10.1 Zmluvné strany vyhlasujú, že konkrétny rozsah činností Tretej strany je daný Zmluvou o službách.

Článok 11

Povinnosti po skončení Zmluvy

- 11.1 Zmluvné strany berú na vedomie, že predmetom plnenia Zmluvy o službách môže byť autorské dielo podľa zákona č. 185/2015 Z.z. Autorský zákon v platnom znení, ktorého súčasťou môže byť:
- 11.1.1 softvér, ktorý bol vytvorený Treťou stranou predovšetkým pre podmienky a potreby Prevádzkovateľa základnej služby;
 - 11.1.2 softvér Tretej strany, ktorý má všeobecný charakter;
 - 11.1.3 softvér tretích osôb; alebo
 - 11.1.4 OpenSource softvér, ktorý je podriadený príslušnej licencií slobodného softvéru.
- 11.2 Zmluvné strany berú ďalej na vedomie, že predmetom plnenia Zmluvy o službách 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.
- 11.3 S ohľadom na body 11.1 a 11.2 Zmluvy Zmluvné strany berú na vedomie, že Tretia strana je v zmysle § 8 ods. 2 písm. p) Vyhlášky povinná po zániku Zmluvy umožniť Prevádzkovateľovi základnej služby zabezpečiť kontinuitu prevádzkovanvej základnej služby vo vzťahu k Službám, ktoré priamo súvisia s prevádzkou tejto základnej služby v rámci sietí a informačných systémov Prevádzkovateľa základnej služby.
- 11.4 Zmluvné strany sa dohodli, že spôsob splnenia povinnosti Tretej strany podľa bodu 11.3 Zmluvy je výlučne na uvážení Tretej strany. Splnenie tejto povinnosti Treťou stranou alebo ďalším dodávateľom určeným Treťou stranou spôsobom podľa predchádzajúcej vety zakladá povinnosť Prevádzkovateľa základnej služby zaplatiť Tretej strane alebo tomuto ďalšiemu dodávateľovi určenému Treťou stranou cenu obvyklú za porovnateľné plnenie, ktoré Prevádzkovateľ základnej služby od Tretej strany alebo ďalšieho dodávateľa určeného Treťou stranou vo vzťahu k plneniu povinnosti podľa bodu 11.3 Zmluvy obdrží.

Článok 12

Zodpovednosť za škodu

- 12.1 Zmluvná strana zodpovedá za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinnosti Zmluvnej strany stanovenej Zákomom alebo Zmluvou. Za škodu vzniknutú Zmluvnej strane sa na účely Zmluvy nepovažuje pokuta alebo akákoľvek iná sankcia uložená Zmluvnej strane príslušným štátnym orgánom.
- 12.2 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 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.
- 12.3 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 na strane porušujúcej Zmluvnej strany a vznikom škody. .
- 12.4 V prípade preukázania existencie príčinnej súvislosti podľa tohto ustanovenia Článok 12 Zmluvy je porušujúca Zmluvná strana povinná uhradiť poškodenej Zmluvnej strane vzniknutú škodu, a to na základe písomnej výzvy poškodenej Zmluvnej strany doručenej porušujúcej Zmluvnej strane na adresu uvedenú v Zmluve, alebo na inú porušujúcou Zmluvnou stranou oznámenú adresu.

Článok 13

Doručovanie

- 13.1 Ak Zmluvou nie je uvedené inak, písomnosti si doručujú Zmluvné strany na:
- 13.1.1 adresu sídla uvedenú v záhlaví Zmluvy, ibaže Zmluvná strana oznámi písomne druhej Zmluvnej strane zmenu adresy;
- 13.2 Písomnosť podľa bodu 13.1.1 Zmluvy sa považuje za doručенú, ak:
- 13.2.1 sa druhá Zmluvná strana o písomnosti nedozvedela, a to dňom, keď sa zásielka vrátila odosielajúcej zmluvnej strane s reláciou poštového podniku Adresát neznámy, neprevzaté v odbernej lehote alebo ak ju adresát odmietol prevziať, a to dňom vrátenia zásielky odosielajúcej zmluvnej strany
- 13.2.2 dňom prevzatia písomnosti alebo dňom odmietnutia prevziať písomnosť pri osobnom doručovaní.
- 13.3 Písomnosť podľa bodu **Chyba! Nenašiel sa žiaden zdroj odkazov.** Zmluvy sa považuje za doručенú, ak Príloha č. 7 Zmluvy neustanovuje inak, druhým dňom odo dňa jej preukázateľného odoslania druhej Zmluvnej strane, a to aj v prípade, ak sa druhá Zmluvná strana o tejto písomnosti nedozvedela.
- 13.4 Písomnosť podľa bodu **Chyba! Nenašiel sa žiaden zdroj odkazov.** Zmluvy sa považuje za doručенú po splnení nasledovných podmienok:
- 13.4.1 písomnosť v podobe elektronickej správy je podpísaná kvalifikovaným elektronickým podpisom osoby alebo osôb oprávnených konať alebo podpisovať za Zmluvnú stranu v súlade so zákonom č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v platnom znení;
- 13.4.2 prijatie elektronickej správy podľa bodu 13.4.1 Zmluvy je druhou Zmluvnou stranou potvrdené.
- 13.5 Pre vylúčenie akýchkoľvek pochybností platí, že písomnosťou sa na účely ustanovenia Článok 13 Zmluvy rozumie akákoľvek informácia alebo údaj, alebo obsah akejkoľvek druhej Zmluvnej strane adresovanej komunikácie bez ohľadu na formu vyhotovenia (papierová, elektronická a pod.).

Článok 14 Záverečné ustanovenia

- 14.1 Zmluva je vyhotovená v dvoch vyhotoveniach. Každá Zmluvná strana dostane po jednom vyhotovení. Neoddeliteľnou súčasťou Zmluvy sú nasledovné Prílohy:
- 14.1.1 Príloha č. 1: Analýza rizík;
- 14.1.2 Príloha č. 2: Bezpečnostné politiky Prevádzkovateľa základnej služby;
- 14.1.3 Príloha č. 3: Zoznam pracovných rolí Tretej strany a ich personálne obsadenie;
- 14.1.4 Príloha č. 4: Bezpečnostné opatrenia;
- 14.1.5 Príloha č. 5: Špecifikácia a rozsah bezpečnostných opatrení;
- 14.1.6 Príloha č. 6: „Vzor“ Mlčanlivost'.
- 14.2 Tretia strana berie na vedomie a akceptuje, že zmluva (vrátane jej príloh) podlieha režimu zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) ako povinne zverejňovaná zmluva a nemá námietky voči zverejneniu akéhokoľvek údaju obsiahnutého v zmluve.
- 14.3 Zmenu obchodného mena, sídla, DIČ, právnej formy, adresy pre poštový styk, čísla účtu, telefónnych čísiel, e-mailovej adresy a mien kontaktných osôb (vrátane osôb oprávnených konať vo veciach technických) nie je potrebné vykonať dodatkom, postačuje jednostranné písomné oznámenie týchto skutočností doručené druhej zmluvnej strane, ktoré bude podpísané oprávnenými zástupcami konajúcej zmluvnej strany. Zmluvné strany sa zaväzujú, že každú zmenu údajov uvedených v predchádzajúcej vete oznámia druhej zmluvnej strane do 10 dní, odkedy ku zmene došlo.
- 14.4 Pokiaľ nie je v Zmluve uvedené inak, riadia sa práva a povinnosti Zmluvných strán Zákonom a Obchodným zákonníkom.

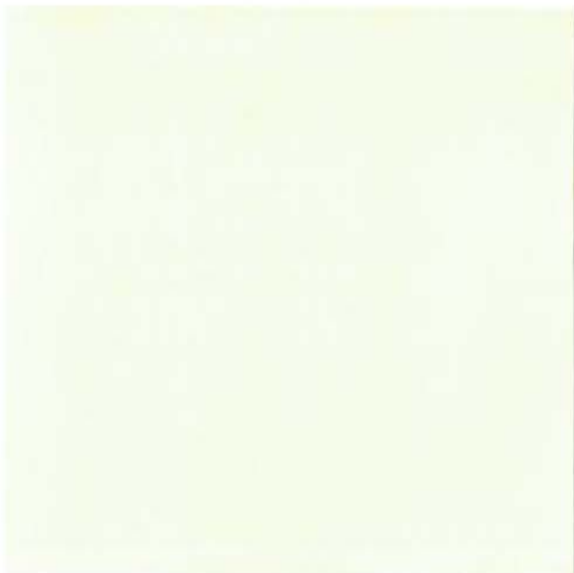
- 14.5 Zmluvu je možné meniť, upravovať alebo dopĺňať iba písomnými dodatkami, ktoré sa po podpísaní obidvoma Zmluvnými stranami stávajú jej neoddeliteľnou súčasťou.
- 14.6 Sporné otázky vyplývajúce zo Zmluvy sa budú prednostne riešiť dohodou Zmluvných strán a až potom, keď sa ich nepodarí vyriešiť dohodou, prostredníctvom súdu. Zmluvné strany si dohodli lehotu 30 dní na vyriešenie sporných otázok dohodou Zmluvných strán. Lehotu podľa predchádzajúcej vety je možné Zmluvnými stranami predĺžiť o ďalších 30 dní.
- 14.7 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.
- 14.8 V prípade Zmluvy a Zmluvy o službách sa jedná o zmluvy vzájomne podmienené.

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 Banskej Bystrici dňa 12.1.2021

V Piešťanoch dňa 17.12.2020

Za Tretiu stranu:



podpredseda predstavenstva

Za Prevádzkovateľa



Ing. Vladimír Púčik
predseda predstavenstva
Trnavská vodárenská spoločnosť a.s.



Príloha č. 1
K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Analýza rizík

Príloha č. 2
K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Bezpečnostné politiky Prevádzkovateľa základnej služby

Príloha č. 3
K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

„Vzor“ Zoznam pracovných rolí Tretej strany a ich personálne obsadenie:

- | | | |
|----|--------------------|--|
| 1) | Meno a priezvisko: | Ľubomír Kopáček |
| | Pracovná rola: | starší špecialista kybernetickej bezpečnosti |
| 2) | Meno a priezvisko: | Martin Fábry |
| | Pracovná rola: | starší špecialista kybernetickej bezpečnosti |
| 3) | Meno a priezvisko: | Lenka Križanová |
| | Pracovná rola: | mladší špecialista |
| 4) | Meno a priezvisko: | Juraj Kočan |
| | Pracovná rola: | mladší špecialista |

Príloha č. 4
K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Bezpečnostné opatrenia

- 1.1 Oblasť technických zraniteľností systémov a zariadení sa zabezpečuje prostredníctvom:
 - 1.1.1 nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí;
 - 1.1.2 nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí;
 - 1.1.3 využívania verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.
- 1.2 Oblasť riadenia bezpečnosti sietí a informačných systémov sa zabezpečuje prostredníctvom:
 - 1.2.1 riadenia prístupov používateľov k sieťam a informačným systémom podľa § 12 Vyhlášky,
 - 1.2.2 riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom;
 - 1.2.3 prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povolené na princípe zásady najnižších privilégií;
 - 1.2.4 bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup (napr. bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov);
 - 1.2.5 opatrenia, že sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete;
 - 1.2.6 opatrenia, že spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov;
 - 1.2.7 serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu;
 - 1.2.8 udržiavania zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave;
 - 1.2.9 použitia automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou;
 - 1.2.10 blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje;
 - 1.2.11 neumožnenia komunikácie a prevádzky aplikácií cez neautorizované porty;
 - 1.2.12 systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete;
 - 1.2.13 implementácie systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky;
 - 1.2.14 smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu;
 - 1.2.15 vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete;
 - 1.2.16 vykonávania pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.
- 1.3 Oblasť riadenia prístupov sa zabezpečuje prostredníctvom nasledovných opatrení:
 - 1.3.1 vypracovania zásad riadenia prístupu k informáciám;
 - 1.3.2 riadenia prístupu používateľov;
 - 1.3.3 vymedzenie príslušných zodpovedností používateľov;

- 1.3.4 riadenia prístupu k sieťam, čím sa rozumie:
- 1.3.4.1. že každému používateľovi siete a informačného systému sa prideliť jednoznačný identifikátor na autentizáciu na vstup do siete a informačného systému;
 - 1.3.4.2. zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov;
 - 1.3.4.3. 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);
 - 1.3.4.4. výkon kontroly prístupových účtov a prístupových oprávnení v pravidelných intervaloch, najmenej však raz za 3 mesiace na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov;
 - 1.3.4.5. určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za pridelenie 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.
- 1.3.5 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.
- 1.3.6 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.
- 1.4 Oblasť riešenia kybernetických bezpečnostných incidentov pozostáva z/zo:
- 1.4.1 Riešenia kybernetických bezpečnostných incidentov, ktoré pozostáva z:
- 1.4.1.1. prípravy a vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov;
 - 1.4.1.2. monitorovania a analyzovania udalostí v sieťach a informačných systémoch;
 - 1.4.1.3. detekcie kybernetických bezpečnostných incidentov;
 - 1.4.1.4. zberu relevantných informácií o kybernetických bezpečnostných incidentoch;
 - 1.4.1.5. vyhodnocovania kybernetických bezpečnostných incidentov;
 - 1.4.1.6. riešenia zistených kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov; a
 - 1.4.1.7. vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatia opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov.
- 1.4.2 Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmenej:
- 1.4.2.1. postup pri internom nahlasovaní kybernetických bezpečnostných incidentov;
 - 1.4.2.2. postup pri hlásení kybernetických bezpečnostných incidentov podľa § 24 ods. 1 Zákona;
 - 1.4.2.3. postup pri riešení jednotlivých typov kybernetických bezpečnostných incidentov a spôsob ich vyhodnocovania; a
 - 1.4.2.4. spôsob evidencie kybernetických bezpečnostných incidentov a použitých riešení.
- 1.4.3 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.
- 1.4.4 Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje:
- 1.4.4.1. zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch;
 - 1.4.4.2. vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom;
 - 1.4.4.3. vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov;
 - 1.4.4.4. revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.
- 1.4.5 Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom:
- 1.4.5.1. pridelenia zodpovednosti a určenia postupov na zvládanie kybernetických bezpečnostných incidentov;
 - 1.4.5.2. zavedenia procesu získavania a uchovávaní podkladov potrebných na analýzu kybernetickej bezpečnostnej udalosti a kybernetického bezpečnostného incidentu;
 - 1.4.5.3. prijímania opatrení na odvrátenie alebo zmiernenie dopadu kybernetického bezpečnostného incidentu;
 - 1.4.5.4. zavedenia procesu nahlasovania kybernetických bezpečnostných incidentov;
 - 1.4.5.5. vedenia záznamov o kybernetických bezpečnostných incidentoch vrátane použitých riešení;
 - 1.4.5.6. prešetrovania a určenia príčin vzniku kybernetického bezpečnostného incidentu aktualizáciou bezpečnostnej stratégie alebo príslušnej bezpečnostnej politiky a prijatia primeraných bezpečnostných opatrení zamedzujúcich jeho opakovanému výskytu; a
 - 1.4.5.7. určenia osoby zodpovednej za nahlasovanie a odovzdávanie hlásení o kybernetických bezpečnostných incidentoch do jednotného informačného systému kybernetickej bezpečnosti, ktoré nastali alebo sa prejavili v rámci siete alebo informačného systému základnej služby.
- 1.4.6 Súčasťou evidencie kybernetických bezpečnostných incidentov sa na zabezpečenie dôkazu alebo dôkazného prostriedku evidujú aj informácie identifikujúce kybernetický bezpečnostný incident, najmä:
- 1.4.6.1. lokalita;
 - 1.4.6.2. hostname;
 - 1.4.6.3. MAC adresy;
 - 1.4.6.4. IP adresy;
 - 1.4.6.5. identifikačné údaje všetkých zariadení a zúčastnených osôb; a
 - 1.4.6.6. dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia.
- 1.5 Oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov:
- 1.5.1 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.
 - 1.5.2 Zhoda sietí a informačných systémov základnej služby s požiadavkami na zabezpečenie kybernetickej bezpečnosti týchto sietí a informačných systémov, monitorovanie účinnosti bezpečnostných opatrení a vyhodnotenie aktuálnosti bezpečnostnej dokumentácie sa zisťuje prostredníctvom auditu kybernetickej bezpečnosti.
 - 1.5.3 Monitorovanie bezpečnosti sietí a informačných systémov sa uskutočňuje implementáciou centrálného nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu:
 - 1.5.3.1. centrálnych sieťových prvkov a serverov;
 - 1.5.3.2. služieb prístupných do externých sietí; a
 - 1.5.3.3. kritických interných serverov a služieb;

- 1.5.4 Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej:
- 1.5.4.1. aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených;
 - 1.5.4.2. 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;
 - 1.5.4.3. pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla;
 - 1.5.4.4. automatické varovné alebo chybové hlásenia systémov;
 - 1.5.4.5. detegované podozrivé alebo škodlivé aktivity; a
 - 1.5.4.6. 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.
- 1.5.5 Prevádzkové záznamy sú zabezpečené najmenej tak, že
- 1.5.5.1. sú čitateľné výlučne osobám povereným ich analýzou;
 - 1.5.5.2. zamedzujú možnosti prepísania alebo vymazania záznamu;
 - 1.5.5.3. záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete;
 - 1.5.5.4. sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

Príloha č. 5
K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Špecifikácia a rozsah bezpečnostných opatrení

Je súčasťou dokumentu Bezpečnostná dokumentácia v zmysle vyhlášky 362/2018

Príloha č. 6
K Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

„Vzor“ Mlčanlivost'

