Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností č. 9309/2025

(ďalej aj len **„Zmluva“**)
v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti
a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
medzi zmluvnými stranami

Objednávateľ:	**Západoslovenská vodárenská spoločnosť, a.s.**
(ďalej aj ako Prevádzkovateľ základnej služby)	
Sídlo:	Nábrežie za hydrocentrálou 4, 949 60 Nitra
Zápis v Obchodnom registri:	OS Nitra, Oddiel: Sro, vl. č.: 10193/N
Konajúci:	PhDr. Mgr. art. Otokar Klein, ArtD. predseda predstavenstva Ing. Marek Illéš člen predstavenstva
BIC:	SUBASKBX
IBAN:	SK66 0200 0000 0000 0260 3112
IČO:	36550949
DIČ:	2020154609
IČ DPH:	SK2020154609
Kontaktná osoba:	
Kontaktný mail pre hlásenie incidentu: kybermanager@zsvs.sk	

a

Poskytovateľ:	**DATACAR spol. s r.o.**
Sídlo:	Piešťl II. č129, 962 12 Detva
Korešpondenčná adresa:	Piešťl II. č129, 962 12 Detva
Zápis v Obchodnom registri:	Okresný súd Banská Bystrica, Oddiel: Sro, Vložka č.: 11839/S
IBAN:	SK06 7500 0000 0040 2317 3199
BIC kód:	CEKOSKBX
IČO:	36 650 811
DIČ:	202210531
IČ DPH:	SK202210531
Kontaktná osoba:	Ing. Maroš Krnáč
Zastúpený:	Ing. Maroš Krnáč, konateľ spoločnosti

(ďalej spolu aj len **„zmluvné strany“**)

Preambula

1. Objednávateľ je v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon“) Prevádzkovateľom základnej služby typu: „Dodávatelia a distribútori vody na pitie, varenie, prípravu potravín alebo iné domáce účely, bez ohľadu na jej pôvod a na to, či bola dodaná z distribučnej siete, cisterny alebo vo fľašiach či nádobách; s výnimkou distribútorov, u ktorých je distribúcia vody iba časťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru, ktorá sa nepovažuje za základnú službu“ v sektore „Voda a atmosféra“, podsektor „Zabezpečovanie pitnej vody“.
2. Objednávateľ je ako Prevádzkovateľ základnej služby v zmysle Zákona, § 19, odstavec 2, povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných technológií Objednávateľa a ktorá je dodávaná treťou stranou – poskytovateľom zmluvnej činnosti, uzatvoriť s treťou stranou túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení, ktoré je tretia strana povinná u seba zabezpečiť a notifikačných povinností voči Objednávateľovi pri vzniku a riešení bezpečnostného incidentu.

Článok I.
Predmet Zmluvy

1. Predmetom tejto Zmluvy je záväzok Poskytovateľa zabezpečovať plnenie bezpečnostných opatrení a notifikačných povinností v zmysle Preambuly tejto Zmluvy vyplývajúci z uzavretia zmluvy s Objednávateľom DATACAR, spol. s r.o.

   (ďalej len „ZoD").

Článok II.
Definícia pojmov

1. Pojmy používané v tejto Zmluve (sieť a informačný systém, kybernetický priestor, kontinuita, dôvernosť, dostupnosť, integrita, kybernetická bezpečnosť, riziko, hrozba, kybernetický bezpečnostný incident, základná služba, prevádzkovateľ základnej služby, riešenie kybernetického bezpečnostného incidentu) majú význam im priradený v Zákone a jeho vykonávacích predpisoch.
2. Zmluvná činnosť – vykonanie a odovzdanie diela, ktorú Poskytovateľ realizuje na základe ZoD.

Článok III.
Obdobie trvania Zmluvy

1. Zmluva sa uzatvára na dobu určitú – na dobu platnosti a účinnosti ZoD.

Článok IV.
Povinnosť Poskytovateľa dodržiavať bezpečnostnú politiku prevádzkovateľa základnej služby a prijať bezpečnostné opatrenia

1. Poskytovateľ sa pri realizácii zmluvnej činnosti vyplývajúcej zo ZoD zaväzuje dodržiavať platné bezpečnostné politiky Prevádzkovateľa základnej služby, ktoré sú pre Poskytovateľa ako Tretiu stranu v zmysle Zákona, normatívne upravené v dokumentoch Prevádzkovateľa základnej služby a sú prílohami k tejto Zmluve.
2. Poskytovateľ vyhlasuje, že sa s bezpečnostnou politikou Prevádzkovateľa základnej služby oboznámil a podpisom tejto Zmluvy vyjadruje súhlas s bezpečnostnou politikou Prevádzkovateľa základnej služby.
3. Poskytovateľ je povinný a zaväzuje sa chrániť všetky informácie ktoré mu Prevádzkovateľ základnej služby poskytol.
4. Poskytovateľ sa zaväzuje vo vlastnej spoločnosti prijať a dodržiavať bezpečnostné opatrenia minimálne v rozsahu podľa Článku V tejto Zmluvy.

Článok V.
Špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma Poskytovateľ a vyjadrenie súhlasu s nimi

Poskytovateľ prijíma bezpečnostné opatrenia vo vlastnej spoločnosti v nasledujúcich oblastiach:

1. Oblasť odhaľovania technických zraniteľností informačných systémov a zariadení, ktoré Poskytovateľ využíva pri poskytovaní služieb – Zmluvnej činnosti - Prevádzkovateľovi základnej služby. Cieľom opatrenia je odhaliť zraniteľnosť informačných systémov a zariadení skôr, než bude zneužitá a prerastie do incidentu. Opatrenie Poskytovateľ realizuje pomocou:
   a. Zavedením a prevádzkou nástrojov určených na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí a technických prostriedkov a ich častí.
   b. Využitím verejných a výrobcami poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2. Oblasť riadenia bezpečnosti sietí a informačných systémov. Cieľom opatrenia je zabrániť útočníkovi prístup k jednotlivým sieťam a informačným systémom ako aj pohyb medzi nimi. Opatrenie Poskytovateľ realizuje pomocou:
    a. Dôslednou segmentáciou a mikrosegmentáciou sietí a informačných systémov.
    b. Riadením prístupu a komunikácie medzi segmentami na princípe zásady najnižších privilégií.
    c. Vo vzdialenom prístupe využívaním dvojfaktorovej autentizácie a/alebo použitím kryptografických prostriedkov.
    d. Využitím blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.
    e. Vykonávaním kontroly na prítomnosť škodlivého kódu v zariadení, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia bezpečnosti pripájaného zariadenia, to je zaplatením zmluvnej pokuty pri preukázaní vzniku incidentu pripojením nebezpečného zariadenia. Pokuty sú uvedené v článku XII.
3. Oblasť riadenia prístupov. Cieľom opatrenia je jednoznačná identifikácia prístupu osôb k sieti a informačným systémom. Opatrenie Poskytovateľ realizuje pomocou:
    a. Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade najnižších privilégií. Používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie jemu zverených úloh používateľa alebo administrátora.
    b. Vypracovaných a používaných zásad 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.
    c. Monitorovaním prístupu a používania informačného systému a riadenia vzdialeného prístupu.
    d. Riadenie procesu prideľovania jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
    e. Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
4. Oblasť riešenia kybernetických bezpečnostných incidentov. Cieľom je detegovať a riešiť kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na výkon činnosti pre Prevádzkovateľa základnej služby. Opatrenie Poskytovateľ realizuje pomocou:
    a. Oboznámením sa s postupmi, ktoré vyžaduje Prevádzkovateľ základnej služby pri riešení kybernetických bezpečnostných incidentov
    b. Monitorovania a analyzovania udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Prevádzkovateľovi základnej služby.
    c. Riešením zistených kybernetických bezpečnostných incidentov a znížením následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Prevádzkovateľa základnej služby.
    d. Vyhodnocovaním kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Prevádzkovateľom základnej služby.
5. Oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov. Cieľom je predchádzanie bezpečnostných incidentov a zlepšovanie bezpečnostných opatrení. Opatrenia Poskytovateľ realizuje podľa § 15 vyhlášky NBÚ č. 362/2018 Z. z., najmä implementovaním centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov a to minimálne pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb Prevádzkovateľovi základnej služby.

Článok VI.
Rozsah činnosti Poskytovateľa

1. Poskytovateľ bude realizovať zmluvné činnosti v rozsahu podľa:
   - Predmetu zmluvy uvedeného v ZoD,
   - Prílohy č. 1 ZoD - Opisu predmetu obstarávania.

Článok VII.
Ďalšie povinnosti Poskytovateľa

1. Poskytovateľ sa zaväzuje poskytnúť Objednávateľovi zoznam pracovných rolí Poskytovateľa s uvedením identifikačných údajov osôb zastávajúcich niektorú z pracovných úloh pri plnení zmluvnej činnosti. Zoznam obsahuje: rola, meno, priezvisko, kontakt (telefón, mail), všetkých osôb, ktoré majú mať prístup do informačných a/alebo technologických infraštruktúr a/alebo k informáciám a údajom Objednávateľa.
2. Poskytovateľ je povinný oznámiť Objednávateľovi každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny.
3. Každá osoba Poskytovateľa zúčastnená na predmete plnenia, vlastnoručne podpisuje vyjadrenie o zachovaní mlčanlivosti podľa § 12 ods. 1 Zákona. Poskytovateľ sa zaväzuje zabezpečiť a odovzdať Objednávateľovi tieto písomné vyjadrenie o zachovávaní mlčanlivosti.

Článok VIII.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u Poskytovateľa

1. Objednávateľ je v zmysle Zákona oprávnený vykonávať kontrolnú činnosť a audit u Poskytovateľa.
2. Objednávateľ je oprávnený vykonať kontrolnú činnosť a audit u Poskytovateľa prostredníctvom osoby, ktorej identifikačné údaje je Objednávateľ povinný Poskytovateľovi včas oznámiť.
3. Objednávateľ je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu pravidelne raz za kalendárny rok; v prípade podozrenia z porušenia tejto Zmluvy alebo Zákona; v prípade nedodržania bezpečnostných opatrení a v prípade žiadosti dozorného orgánu podľa Zákona.
4. Objednávateľ informuje o termíne vykonania auditu alebo kontroly Poskytovateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 dní pred vykonaním auditu alebo kontroly. Poskytovateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 dní odo dňa zaslania oznámenia. Pokiaľ Poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.
5. Práva a povinnosti zmluvných strán pri realizácii auditu:
   a. Objednávateľ je oprávnený vykonať u Poskytovateľa audit zameraný na overenie plnenia povinností Poskytovateľa podľa tejto Zmluvy a efektívnosti ich plnenia.
   b. Prípadné nedostatky zistené auditom je Poskytovateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
   c. Objednávateľ môže audit u Poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Objednávateľa pri výkone auditu realizuje Objednávateľom poverená tretia osoba.
   d. Poskytovateľ je povinný pri audite spolupracovať s Prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti v rozsahu podľa tejto Zmluvy.
   e. Objednávateľ je v rámci auditu oprávnený klásť otázky zamestnancom Poskytovateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
   f. Vykonanie alebo nevykonanie auditu Objednávateľom nezbavuje Poskytovateľa zodpovednosti za plnenie povinností Poskytovateľa vyplývajúcich z tejto Zmluvy.
   g. Ak Poskytovateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
   h. Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

i. Objednávateľ a jeho zamestnanci pri návšteve priestorov Poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny Poskytovateľa týkajúce sa uvedených priestorov na úseku BOZP a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO"), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Poskytovateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Poskytovateľa.

6. Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť Objednávateľovi na účely kontroly a auditu v zmysle ust. § 28 a 29 Zákona.

Článok IX.
Podmienky a možnosti zapojenia ďalšieho Poskytovateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto Poskytovateľa a podmienky a možnosti zapojenia subPoskytovateľa prostredníctvom Poskytovateľa.

1. Poskytovateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb Prevádzkovateľovi základnej služby nového Poskytovateľa bez predchádzajúceho výslovného písomného súhlasu Prevádzkovateľa základnej služby.
2. Ak Poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb Prevádzkovateľovi základnej služby nového Poskytovateľa, tomuto novému Poskytovateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Zmluve Poskytovateľovi. Zodpovednosť voči Prevádzkovateľovi základnej služby nesie Poskytovateľ, ak nový Poskytovateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

Článok X.
Povinnosť Poskytovateľa hlásiť kybernetický bezpečnostný incident a ďalšie informácie prevádzkovateľovi základnej služby vrátane povinností Poskytovateľa pri riešení kybernetického bezpečnostného incidentu

1. Poskytovateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident v zmysle Zákona a informovať Prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.
2. Poskytovateľ informuje Prevádzkovateľa základnej služby zaslaním hlásenia o kybernetickom bezpečnostnom incidentu na e-mailovú adresu uvedenú v záhlaví tejto Zmluvy.
3. Hlásenie musí obsahovať:
    a. informácie o tom, kto hlási kybernetický bezpečnostný incident:
        - identifikačné údaje Poskytovateľa,
        - funkcia a pracovné zaradenie osoby Poskytovateľa, ktorá hlási kybernetický bezpečnostný incident,
        - identifikačné údaje ďalších organizácií, ktoré boli ešte dotknuté kybernetickým bezpečnostným incidentom u Poskytovateľa,
    b. informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu:
        - typ závažného kybernetického bezpečnostného incidentu

- nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
- škodlivý kód (vírus, malvér, ransomvér),
- získavanie informácií (skenovanie siete, odpočúvanie, sociálne inžinierstvo),
- pokus o prienik do systému,
- 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),
- zraniteľnosť (ich existencia),
- iné,

– časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu
  - čas začiatku incidentu (ak je známy), čas a spôsob zistenia incidentu, informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,

– detailný opis priebehu závažného kybernetického bezpečnostného incidentu a jeho prvotná príčina,
– popis rozsahu škôd,

c. informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom:
   – prvotne zasiahnuté aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby,
   – informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity služby alebo činnosti, a či je zariadenie v čase podávania hlásenia v prevádzke.

4. Poskytovateľ je povinný hlásiť Prevádzkovateľovi základnej služby ďalšie informácie, ktoré Prevádzkovateľ základnej služby potrebuje na plnenie svojej povinností vyplývajúcich zo Zákona, najmä:
   a. informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
   b. informácie potrebné na účely splnenia povinnosti Prevádzkovateľa základnej služby v zmysle ust. § 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,
   c. informácie v potrebnom rozsahu na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 27 ods.10 Zákona.
5. Prevádzkovateľ základnej služby je oprávnený požadovať od Poskytovateľa návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu, a to najmä v prípadoch, kedy Národný bezpečnostný úrad požaduje od prevádzkovateľa základnej služby návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu /ďalej aj len „ochranné opatrenie"/. Ochranné opatrenie je prijímané na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

Článok XI.
Podmienky a spôsob ukončenia Zmluvy

1. Zmluvné strany môžu túto Zmluvu ukončiť vždy písomnou dohodou zmluvných strán; Zmluva zaniká dňom dohodnutým v písomnom vyhotovení dohody o ukončení tejto Zmluvy, nikdy nie pred uplynutím účinnosti ZoD s Objednávateľom. V prípade, ak zmluvné strany dohodnú deň ukončenia Zmluvy pred dňom uplynutia účinnosti ZoD, táto Zmluva zaniká súčasne so zánikom účinnosti ZoD.
2. Prevádzkovateľ základnej služby je oprávnený písomne odstúpiť od tejto Zmluvy v prípade, ak Poskytovateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy:

a. Poskytovateľ neodôvodnene odmietne výkon kontrolnej činnosti a auditu prevádzkovateľom základnej služby,
b. Poskytovateľ postúpi svoje práva a povinnosti na ďalšieho Poskytovateľa v rozpore s touto Zmluvou,
c. na majetok Poskytovateľa je vyhlásený konkurz, exekúcia, Poskytovateľ vstúpil do likvidácie, preruší, alebo iným spôsobom ukončí svoju podnikateľskú činnosť,
d. Poskytovateľ, alebo osoba oprávnená konať v jeho mene je právoplatne odsúdená za trestný čin spáchaný v súvislosti s výkonom jeho činnosti, alebo s podnikaním,
e. Poskytovateľ stratí predpoklady na plnenie tejto Zmluvy.

3. Výpovedná lehota je jeden mesiac a začína plynúť prvého dňa mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.
4. Poskytovateľ je povinný po ukončení Zmluvy vrátiť, previesť alebo rozhodnutím Objednávateľa zničiť všetky informácie, ku ktorým mal ako tretia strana počas trvania zmluvného vzťahu prístup.
5. Poskytovateľ je povinný po ukončení Zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok Poskytovateľa ostáva v platnosti aj po ukončení Zmluvy po dobu 5 rokov.
6. Ukončením tejto Zmluvy je Objednávateľ oprávnený ukončiť aj ZoD, ku ktorej je táto Zmluva viazaná.

Článok XII.
Sankcie, zmluvné pokuty a náhrada škody

1. V prípade, ak Poskytovateľ poruší svoje povinnosti v zmysle tejto Zmluvy voči Prevádzkovateľovi základnej služby, a to najmä povinnosť
   a. dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
   b. prijímať a dodržiavať bezpečnostné opatrenia minimálne v rozsahu špecifikovanom v Článku V tejto Zmluvy,
   c. umožniť Prevádzkovateľovi základnej služby vykonať audit Poskytovateľom prijatých bezpečnostných opatrení, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení Poskytovateľom s bezpečnostnou politikou Prevádzkovateľa základnej služby,
   d. nedodržania lehoty 30 pracovných dní odo dňa zistenia nesúladu Poskytovateľom prijatých bezpečnostných opatrení zistených vykonaním auditu u Poskytovateľa na zabezpečenie nápravy nesúladu so Zákonom,
   e. oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny,
   f. zabezpečiť a odovzdať Prevádzkovateľovi základnej služby písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia,

   vzniká prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 30.000,- EUR.
2. Prevádzkovateľ základnej služby je oprávnený uplatniť si zmluvné pokuty a náhradu škody kedykoľvek v priebehu plnenia predmetu Zmluvy, ako aj po zániku Zmluvy v prípade, ak porušenie zmluvných podmienok stanovených touto Zmluvou zistí po zániku zmluvného vzťahu vyplývajúceho zo Zmluvy.
3. V prípade, ak Dodávateľ poruší svoje povinnosti podľa čl. XI. ods. 5. tejto Zmluvy, vzniká Prevádzkovateľovi základnej služby nárok na zaplatenie zmluvnej pokuty vo výške 100.000,- EUR.
4. Uplatnením ktorejkoľvek zmluvnej pokuty alebo zmluvných pokút v zmysle tohto článku nie je dotknutý nárok Prevádzkovateľa základnej služby na náhradu vzniknutej škody v celom rozsahu a právo na uplatnenie ďalšej zmluvnej pokuty podľa tejto Zmluvy. Prevádzkovateľ základnej služby môže uplatňovať náhradu škody a zmluvnej pokuty kumulatívne, Prevádzkovateľ základnej služby má nárok na zaplatenie zmluvnej pokuty a súčasne náhrady škody v plnom rozsahu. Prevádzkovateľ základnej služby je oprávnený jednostranne započítať voči Poskytovateľovi svoje pohľadávky vzniknuté z titulu zmluvnej pokuty a/alebo náhrady škody uplatnenej podľa tejto Zmluvy.

Článok XIII.
Záverečné ustanovenia

1. Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpisu ostatnou zo zmluvných strán.
2. Táto Zmluva sa vyhotovuje v troch rovnopisoch, 2 x pre Prevádzkovateľa základnej služby a 1 x pre Poskytovateľa. Akékoľvek dodatky a zmeny tejto Zmluvy sú platné len v písomnej forme, po ich odsúhlasení a podpísaní oboma zmluvnými stranami.
3. Neoddeliteľnou súčasťou tejto zmluvy sú tieto Prílohy:
   Príloha č.1 Všeobecné požiadavky na fyzickú a informačnú bezpečnosť
   Príloha č.2 Postupy hlásenia kybernetických bezpečnostných incidentov voči PZS
   Príloha č.3 Vzor - HLÁSENIE KYBERNETICKÉHO BEZPEČNOSTNÉHO INCIDENTU.
4. V prípade, že sa niektoré z ustanovení tejto Zmluvy stane neplatným, zmluvné strany sa zaväzujú nahradiť neplatné ustanovenie ustanovením platným tak, aby zodpovedalo účelu tejto Zmluvy a najmä vôli zmluvných strán pri uzatváraní tejto Zmluvy. Zostávajúce ustanovenia Zmluvy sú takouto zmenou nedotknuté.
5. Táto Zmluva sa riadi právnym poriadkom Slovenskej republiky, najmä ustanoveniami Obchodného zákonníka, zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení a vyhláškou č. 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
6. Zmluvné strany vyhlasujú, že ich zmluvná voľnosť nebola žiadnym spôsobom obmedzená.
7. Zmluvné strany vyhlasujú, že táto Zmluva nebola uzavretá v tiesni ani za nápadne nevýhodných podmienok a ani v omyle.
8. Zmluvné strany vyhlasujú, že sú plne spôsobilé k právnym úkonom, že text tejto Zmluvy je určitým a zrozumiteľným vyjadrením ich vážnej a slobodnej vôle byť ňou viazaný, a že si Zmluvu pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom k nej pripájajú svoje vlastnoručné podpisy.

V Nitre, dňa 05 -03- 2025 ...

Objednávateľ:
Západoslovenská vodárenská spoločnosť, a.s.

.....
PhDr. Mgr. art. Otokar Klein, ArtD.
predseda predstavenstva

Ing. Marek Illéš
člen predstavenstva

V Detve, dňa 05 -03- 2025 .....

Poskytovateľ:
DATACAR, spol. s r.o.

tel.: 045/5469 432, mob.: 0902 927 927
.....
Ing. Maroš Krnáč
Konateľ spoločnosti

„Interné“

„RIADENÝ DOKUMENT“
„Elektronická dokumentácia je platná bez podpisu!“

BEZPEČNOSTNÁ POLITIKA PRE TRETIE STRANY

SM 05 – PRÍLOHA Č.1

VŠEOBECNÉ POŽIADAVKY NA FYZICKÚ A INFORMAČNÚ BEZPEČNOSŤ

	Vydal a spracoval	**Kontroloval**	**Schválil**
Meno a priezvisko	Ing. Peter Matej		
Funkcia	MKB		
Dátum	27.2.2022		
Podpis			

*Pozn.: ostatný výtlačok zo siete je neriadený dokument

Zoznam zmien

Zmena č.	Strana	Charakteristika zmeny	Dátum	Meno a priezvisko - podpis
1			Platnosť od:	Vydal: Schválil:
2			Platnosť od:	Vydal: Schválil:
3			Platnosť od:	Vydal: Schválil:
4			Platnosť od:	Vydal: Schválil:
5			Platnosť od:	Vydal: Schválil:
6			Platnosť od:	Vydal: Schválil:
7			Platnosť od:	Vydal: Schválil:
8			Platnosť od:	Vydal: Schválil:
9			Platnosť od:	Vydal: Schválil:
10			Platnosť od:	Vydal: Schválil:

OBSAH:

ZOZNAM POUŽITÝCH SKRATIEK A POJMOV

Skratky

KBaIB	-	kybernetická bezpečnosť a informačná bezpečnosť
MKB	-	manažér kybernetickej bezpečnosti
ZsVS	-	Západoslovenská vodárenská spoločnosť, a. s.
OZ	-	organizačná zložka podniku - odštepný závod
IKT	-	Informačno-komunikačné technológie
IT	-	Informačné technológie
OT	-	Operačné technológie (dispečing a ASRTP)
MFA	-	Multifaktorová autentifikácia prístupu

Pojmy

Predkladateľ zmluvy	-	OZ, úsek/útvar, ktorý objednáva, kontroluje a preberá dielo alebo činnosť vykonávanú pre ZsVS na základe zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb a pod.
Zákon	-	zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zmluva	-	zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
Tretia strana	-	zmluvný partner – zhotoviteľ alebo poskytovateľ služby a prípadne jeho subdodávateľ, na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov ZsVS

1. ÚČEL A CIELE DOKUMENTU

Dokument „Bezpečnostná politika pre tretie strany SM-05 – Príloha č.1“ je súčasťou bezpečnostných opatrení, ktoré popisujú riadenie vzťahov s tretími stranami v zmysle Zákona. Upravuje bezpečnostné politiky, ktorými sú tretie strany povinné sa riadiť v zmysle požiadavky § 20, ods. 3 písmeno e) Zákona. Tieto bezpečnostné politiky upravujú:

a) všeobecné bezpečnostné opatrenia a politiky platné pre tretie strany,
b) vstup tretích strán do objektov ZsVS,
c) pohyb tretích strán po objektoch ZsVS,
d) požiadavky pre pripájanie IKT tretích strán do infraštruktúry ZsVS on-line a on-site spôsobom,
e) spôsob realizácie servisných zásahov tretích strán na IKT ZsVS,
f) spôsob hlásenia bezpečnostných incidentov.

Dokument je tiež prílohou Zmluvy, ktorú je ZsVS ako Prevádzkovateľ základnej služby povinná v zmysle § 19, ods. 2 Zákona pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných technológií ZsVS, s treťou stranou uzatvoriť.

2. ROZSAH PLATNOSTI

Dokument je platný a záväzný pre každú tretiu stranu, ktorá vykonáva činnosti alebo práce na základe zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb alebo inej zmluvy na objektoch IKT v IT alebo OT infraštruktúry ZsVS a pre každého zamestnanca ZsVS, ktorý je poverený sprevádzaním tretej strany, riadením alebo koordinovaním servisných činností tretej strany na IT alebo OT infraštruktúre ZsVS.

3. ZODPOVEDNOSTI A SPOLUPRÁCA

ZsVS zodpovedá za prijatie postupov týkajúcich sa kybernetickej a informačnej bezpečnosti, spracovaných podľa smernice riadenia ISMS dokumentácie a preukázateľné oboznámenie sa všetkých zamestnancov ZsVS s obsahom bezpečnostnej dokumentácie.

MKB vyhodnocuje riziko prístupu tretej strany do infraštruktúry ZsVS, posudzuje rozsah aplikovania zmien na prvkoch infraštruktúry z pohľadu kybernetickej bezpečnosti, vyhodnocuje riziká a incidenty.

Predkladateľ zmluvy s treťou stranou je zodpovedný za komunikáciu s MKB pre posúdenie rozsahu aplikovaných bezpečnostných opatrení pre tretiu stranu a za preukázateľné oboznámenie tretej strany s týmto dokumentom.

4. BEZPEČNOSTNÁ POLITIKA PRE TRETIE STRANY

Tretia strana je povinná informovať všetkých svojich zamestnancov, ktorí budú realizovať zmluvné zásahy na systémoch a zariadeniach ZsVS o povinnosti dodržiavania bezpečnostných opatrení v zmysle tohto dokumentu.

4.1. Všeobecné bezpečnostné požiadavky

4.1.1. Proaktívne pôsobenie tretej strany v oblasti KBaIB

Tretia strana je povinná proaktívne sledovať vývoj v bezpečnostnej oblasti produktov, ktoré vyvíja a dodáva. Sledovať bezpečnosť vývojových nástrojov, používaných softvérových knižníc, aplikovanie vývojových postupov, ktoré minimalizujú zraniteľnosti vyvíjaných a dodávaných produktov. V prípade, že zistí, že jej produkt, alebo služba obsahuje nečakanú zraniteľnosť, je povinná o tom bezodkladne po zistení informovať ZsVS mailom a telefonicky prostredníctvom vedúceho Útvaru IT alebo vedúceho Útvaru dispečingu a tiež mailom informovať MKB na mailovej adrese kybermanager@zsvs.sk.

Informácia musí obsahovať:

- o akú zraniteľnosť sa jedná (kedy bola zistená, označenie, rozsah, dopady zraniteľnosti)
- či existuje na zraniteľnosť záplata, alebo dočasné riešenie
- návrh na aplikovanie záplaty alebo dočasného riešenia

4.1.2. Bezpečnostné opatrenia na strane tretej strany

Tretia strana je povinná prijať bezpečnostné opatrenia vo vlastnej spoločnosti a to v oblastiach:

- Odhaľovanie technických zraniteľností systémov a zariadení, ktoré vyvíja a dodáva
- Riadenie bezpečnosti siete a informačných systémov
- Riadenie prístupov do vlastných sietí a zariadení
- Riešenie kybernetických bezpečnostných incidentov

Rozsah opatrení pre uvedené oblasti je uvedený v Zákone a tiež v Zmluve, ktorú ZsVS ako prevádzkovateľ základnej služby podpisuje s treťou stranou.

4.2. Vstup do objektov ZsVS

Tretie strany sa pri vstupe do objektov ZsVS povinne registrujú na určenom mieste. Za registráciu tretej strany zodpovedá strážna služba, ak je pri vchode do objektu zriadená. Ak strážna služba nie je zriadená, zodpovedá za registráciu tretej strany vedúci pracovník objektu alebo pracovník poverený sprevádzaním tretej strany po objekte.
Každý vstup tretej strany musí byť zaznamenaný, pričom sa zaznamenáva:

- Meno a priezvisko
- Obchodné meno tretej strany
- Čas príchodu
- Čas odchodu
- Činnosť, ktorá bola na IKT realizovaná
- Sprevádzajúca/dozorujúca osoba

4.3. Pohyb v objektoch ZsVS

Tretie strany vykonávajúce servisné činnosti alebo iné práce na IT alebo OT infraštruktúre ZsVS sa v objektoch ZsVS môžu pohybovať len v sprievode povereného zamestnanca ZsVS.

Vytváranie fotografického a filmového záznamu je všeobecne zakázané, výnimky sú špecificky upravené pre jednotlivé bezpečnostné zóny. Vykonávanie záznamu v objektoch je možné vždy len po predchádzajúcom písomnom odsúhlasení ZsVS a v koordinácii s povereným zamestnancom ZsVS. Vykonávanie záznamu správania sa IKT je možné len po predchádzajúcom písomnom odsúhlasení vedúceho Útvaru IT alebo vedúceho Útvaru dispečingu.

4.4. Pripájanie IKT tretích strán do IT a OT infraštruktúry ZsVS

V prípade, že činnosť tretej strany vyžaduje pripojenie sa do systému alebo zariadenia, musí byť táto požiadavka formulovaná v zmluve o dielo, servisnej zmluvy, zmluve o poskytovaní služieb alebo inej zmluvy na základe, ktorej vykonáva tretia strana činnosť alebo dielo pre ZsVS . Príslušný útvar ZsVS vytvorí prístupové práva pre tretiu stranu. Prístupové práva sú evidované v rozsahu:

- Identifikačné údaje pracovníka tretej strany (Meno a Priezvisko)
- Názov účtu

- Oprávnenia účtu
- Dátum vytvorenia účtu
- Aktívum (IS, zariadenie), na ktorom je účet vytvorený
- Dĺžka platnosti účtu (pokiaľ je to účet s obmedzenou platnosťou)

Po ukončení trvania zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb alebo inej zmluvy uzatvorenej s treťou stranou, príslušný útvar ZsVS odoberie prístupové práva všetkým relevantným účtom.
V prípade mimoriadnej udalosti, ktorá na základe zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb alebo inej zmluvy uzatvorenej s treťou stranou umožňuje okamžité odobratie prístupových práv, tak príslušný útvar odoberie prístupové práva konkrétnej osobe tretej strany hneď po zistení mimoriadnej udalosti. Za mimoriadnu udalosť sa považuje porušenie zmluvných podmienok pre prístup do interných systémov ZsVS.
Všetky prístupy musia byť jedinečné, nie je povolené používanie tzv. skupinových účtov.

Prístupy sa realizujú na konkrétny systém alebo zariadenie, na ktoré je podpísaná zmluva o dielo, servisná zmluva, zmluva o poskytovaní služieb alebo iná zmluva uzatvorená s treťou stranou. Tretia strana nesmie zneužiť poskytnutý prístup na prístupy k iným systémom alebo zariadeniam. Ak tretia strana zistí, že má iný prístup ako je pre realizovanie jej činnosti adekvátny, je povinná na to upozorniť svojho priameho nadriadeného a vedúceho Útvaru IT alebo Útvaru dispečingu ZsVS.

4.4.1. On-line prístup

Ak je to technicky možné, zriaďuje sa prístup s MFA overením prístupu. Za zriadenie bezpečného prístupu je zodpovedný Útvar IT ZsVS. Tretia strana je zodpovedná za bezpečnosť prostredia, z ktorého pristupuje do infraštruktúry ZsVS:

- Čistota zariadenia (notebook, PC, smart zariadenie), z ktorého tretia strana pristupuje. Zariadenie musí obsahovať čerstvé bezpečnostné záplaty, mať funkčný antivírový systém a ďalšie bezpečnostné aplikácie, ktoré garantujú, že tretia strana cez svoje zariadenie, z ktorého pristupuje do infraštruktúry ZsVS nebude hrozbou pre kybernetickú bezpečnosť ZsVS.
- Bezriziková sieť, alebo WiFi, z ktorej tretia strana pristupuje do infraštruktúry ZsVS. Je zakázané pristupovať do infraštruktúry ZsVS prihlasovaním sa z nezabezpečených WiFi sietí.
- Všetky on-line prístupy musia byť monitorované.

4.4.2. On-site prístup

Pripojenie cudzieho zariadenia do vnútornej infraštruktúry ZsVS je zakázané. Pripojenie notebooku, smart zariadenia, WiFi smerovača či akýchkoľvek vopred neschválených zariadení je zakázané.

Pokiaľ je zmluvne dohodnuté, že tretia strana môže pripojiť vlastné zariadenie do infraštruktúry ZsVS, preberá tretia strana plnú zodpovednosť za hrozbu možného nakazenia siete ZsVS jeho zariadením a tiež zodpovedá za čistotu všetkých zariadení a pamäťových médií, ktoré použije (USB, CD, DVD, pamäťové karty a iné).

O pripojení cudzieho zariadenia musí byť realizovaný záznam (písomný alebo elektronický). Záznam vytvorí pracovník ZsVS poverený sprevádzaním tretej strany po objekte ZsVS a do 24 hodín ho doručí (v papierovej forme, alebo mailom) vedúcemu Útvaru IT. Záznam musí obsahovať:

- Dátum a čas pripojenia a odpojenia zariadenia
- Typ zariadenia (hardvér, softvér) alebo použitého pamäťového média
- Dôvod pripojenia (realizovaná činnosť)
- Vlastník zariadenia (tretia strana, Meno a Priezvisko)

4.5. Realizácia servisných zásahov

4.5.1 Aplikovanie zmien na IKT - Upgrade a update

Aplikovanie zmien na IKT (nová verzia, funkčná alebo bezpečnostná záplata, náhrada zariadenia, funkčná zmena a pod.) sa musí realizovať nasledovným spôsobom:

- Tretia strana pred realizáciou zmeny pripraví zoznam krokov, ktoré majú byť počas aplikovania zmeny vykonané, tzv. protokol o realizovaní zmeny. Posledným krokom v protokole je odsúhlasenie, že funkcionalita systému, na ktorom bola zmena realizovaná, nie je narušená a je v zhode s očakávaniami, prezentovanými treťou stranou pred implementáciou zmeny. Tretia strana je povinná si vyžiadať určenie pracovníka ZsVS, ktorý je bude spôsobilý posúdiť funkčnosť systému po realizácii zmeny a podpíše protokol o realizácii zmeny.
- V zozname krokov musia byť špecificky uvedené kroky, ktoré môžu spôsobiť problém (pokiaľ to dokumentácia výrobcu špecificky uvádza ako upozornenie, alebo to vyplýva zo skúseností tretej strany, že pri danom kroku sa môže objaviť špecifický problém, špecifickým problémom môže byť neočakávané správanie sa systému, jeho nečakaný výpadok a znefunkčnenie sekundárnych IKT systémov, ktoré sú na ňom závislé)
- V každom kroku musí byť jasne uvedené, aký je návratový proces v prípade neúspešnej realizácie zmeny
- V prípade požiadavky na odstávku systému alebo jeho časti je potrebné uviesť ako dlho sa odstávka očakáva, ako súvisí s okolitým IKT prostredím, čo ovplyvní činnosť ostatných systémov, aký dopad to bude mať na okolité IKT prostredie
- Musí byť uvedená očakávaná dĺžka odstávky
- Tretia strana zároveň uvedie možné dočasné riziká (zníženie bezpečnosti, dostupnosti, integrity) počas realizácie zmeny
- Realizácia zmeny podlieha schváleniu vedúcim Útvaru IT v prípade realizácie zmien na IT infraštruktúre alebo vedúcim Útvaru dispečingu v prípade realizácie zmien na OT infraštruktúre

- V prípade, že sa zmena dotýka IT aj OT prostredia navzájom, schvaľujú realizáciu zmien oba útvary v konsenze
- V prípade, že tretia strana uvedie v popise realizácie zmeny výskyt možných bezpečnostných rizík, posudzuje realizáciu zmeny MKB
- V prípade, že pri realizácii zmeny dôjde k nečakanej udalosti, je tretia strana povinná udalosť analyzovať a navrhnúť opatrenia pre pokračovanie zmeny, alebo pre roll-back, teda pre návrat do pôvodného stavu pred realizáciou zmeny. Súčasťou analýzy musia byť aj bezpečnostné dopady. V prípade pochybností sa rozhodnutie vykoná konsenzom vedúcich útvaru IT a dispečingu, tretej strany a MKB.
- Po realizácii zmeny musí prebehnúť kontrola funkčnosti
- Zmena je považovaná za úspešne realizovanú, až keď poverený pracovník ZsVS (uvedený na protokole o realizovanej zmene) podpisom protokolu potvrdí, že systém/zariadenie má po zmene očakávanú funkčnosť
- V prípade neúspešnej realizácie zmeny je tretia strana povinná vyhodnotiť neúspešnosť, určiť, v ktorom kroku došlo k zlyhaniu a prečo a navrhnúť nové riešenie. Dátum a čas pre realizáciu nového riešenia je dohodnutý v zmysle príslušnej zmluvy, alebo ak to zmluva neurčuje, tak na základe dohody medzi realizátorom zmeny a povereným pracovníkom zodpovedným za realizáciu zmeny na strane ZsVS. Cieľom je minimalizovať počet neúspešných realizácií zmien na IKT v IT a OT a predchádzať vzniku incidentov spôsobených opakovanou neúspešnou realizáciou zmeny.
- Každá opakovaná zmena po neúspešnej realizácii sa riadi vyššie popísaným postupom.

4.5.2 Aplikovanie zmien na IKT – Urgentné zásahy

V prípade, že realizácia zmeny nie je plánovaná (výpadok služby, zariadenia) riadi sa zásah na základe podpísanej zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb alebo inej zmluvy uzatvorenej s treťou stranou (reakčný čas). Tretia strana vykonáva zásah podľa svojho najlepšieho vedomia. V prípade, že má podozrenie na bezpečnostný problém, informuje o tom neodkladne vedúceho Útvaru IT alebo vedúceho Útvaru dispečingu a MKB.

Po realizácii zásahu tretia strana vypracuje do 5 pracovných dní krátky protokol, v ktorom uvedie:

- Čo bolo príčinou výpadku služby alebo zariadenia
- Aké opatrenia boli realizované, aby bola služba alebo zariadenie opäť funkčné
- Aké opatrenia tretia strana odporúča na predchádzanie podobných výpadkov

V prípade, že dôvodom bol bezpečnostný problém, alebo výpadok mohol byť rizikový pre dôvernosť alebo integritu dát, tretia strana bude odporúčania konzultovať s MKB.

4.5.3 Aplikovanie bezpečnostných záplat

Bezpečnostné záplaty môžu byť plánované (súvisiace s pravidelnou údržbou služby alebo zariadenia – prípad, keď výrobca v pravidelných intervaloch vydáva záplaty – napr. Microsoft), alebo neplánované záplaty, ktoré je potrebné realizovať v mimoriadnych prípadoch, keď sa bezpečnostný problém objaví a je potrebná rýchla reakcia tretej strany.

Aplikovanie neplánovanej bezpečnostnej záplaty je považované za servisný zásah najvyššej priority a očakáva sa od tretej strany urgentný zásah.

4.6. Riadenie incidentov

Za bezpečnostný incident je možné považovať udalosť, ktorá spôsobila narušenie bezpečnosti informačného systému, tzn. že došlo ku strate diskrétnosti, integrity alebo dostupnosti dát alebo služby. Za bezpečnostný incident treba považovať aj odhalený pokus o prekonanie bezpečnostných opatrení. Príklady možných incidentov sú napr. odmietnutie služby, škodlivý kód, neautorizovaný prístup, nevhodné použitie, napadnutie PC vírusom, a pod.

V prípade, že kybernetický incident vznikne v infraštruktúre tretej strany, ktorá má on-line prístupy do infraštruktúry ZsVS, je tretia strana povinná okamžite informovať MKB ZsVS o vzniknutej udalosti a to spôsobom a v rozsahu podľa článku X. Zmluvy.

V prípade, že kybernetický incident vznikne pôsobením tretej strany na infraštruktúre ZsVS, je tretia strana povinná vznik incidentu okamžite ohlásiť vedúcemu Útvaru IT alebo vedúcemu Útvaru dispečingu, sprevádzajúcemu resp. dozorujúcemu zamestnancovi ZsVS a informovať MKB.

MKB vyhodnotí závažnosť incidentu a postupuje v zmysle § 24 Zákona.

5. REGISTER SÚVISIACICH DOKUMENTOV

Zmluva
Zonácia vodohospodárskych objektov
Riadenie bezpečnostných incidentov

6. ZMENOVÉ RIADENIE A PLATNOSŤ

Tento dokument nadobúda účinnosť dňom jeho schválenia predstavenstvom ZsVS. Jeho aktualizácia sa vykonáva podľa potreby, revízie sa vykonávajú minimálne 1 x za 2 roky. Zodpovednosť za zmeny a právo kontroly dodržovania ustanovení tejto smernice má MKB. Doba platnosti nie je obmedzená.

7. ZOZNAM PRÍLOH

„Interné“

„RIADENÝ DOKUMENT“
„Elektronická dokumentácia je platná bez podpisu!“

BEZPEČNOSTNÁ POLITIKA PRE TRETIE STRANY

SM 05 – PRÍLOHA Č. 2

POSTUPY HLÁSENIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV VOČI PZS

	Vydal a spracoval	**Kontroloval**	**Schválil**
Meno a priezvisko	Ing. Peter Matej		
Funkcia	MKB		
Dátum	28.2.2022		
Podpis			

*Pozn.: ostatný výtlačok zo siete je neriadený dokument

Zoznam zmien

Zmena č.	Strana	Charakteristika zmeny	Dátum	Meno a priezvisko - podpis
1			Platnosť od:	Vydal:
				Schválil:
2			Platnosť od:	Vydal:
				Schválil:
3			Platnosť od:	Vydal:
				Schválil:
4			Platnosť od:	Vydal:
				Schválil:
5			Platnosť od:	Vydal:
				Schválil:
6			Platnosť od:	Vydal:
				Schválil:
7			Platnosť od:	Vydal:
				Schválil:
8			Platnosť od:	Vydal:
				Schválil:
9			Platnosť od:	Vydal:
				Schválil:
10			Platnosť od:	Vydal:
				Schválil:

OBSAH:

ZOZNAM POUŽITÝCH SKRATIEK a POJMOV

Skratky

KBaIB	-	kybernetická bezpečnosť a informačná bezpečnosť
MKB	-	manažér kybernetickej bezpečnosti
ZsVS	-	Západoslovenská vodárenská spoločnosť, a.s
IKT	-	Informačno-komunikačné technológie
IT	-	Informačné technológie
OT	-	Operačné technológie (dispečing a ASRT)
MFA	-	Multifaktorová autentifikácia prístupu
KBI	-	Kybernetický bezpečnostný incident
PZS	-	Prevádzkovateľ základnej služby v zmysle Zákona
VPN	-	Virtual Private Network – prepojenie sietí šifrovaným spôsobom

Pojmy

Predkladateľ zmluvy	-	OZ, úsek/útvar, ktorý objednáva, kontroluje a preberá dielo alebo činnosť vykonávanú pre ZsVS na základe zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb a pod.
Zákon	-	zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
On-line	-	vzdialený prístup, prístup pri ktorom je dodávateľ mimo objektu ZsVS a pripája sa cez internet k prvkom IKT infraštruktúry ZsVS
On-site	-	realizácia servisnej činnosti priamo v objektoch ZsVS
Zmluva	-	zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
Tretia strana	-	zmluvný partner – zhotoviteľ alebo poskytovateľ služby a prípadne jeho subdodávateľ, na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov ZsVS

1. ÚČEL A CIELE DOKUMENTU

Dokument „Bezpečnostná politika pre tretie strany SM-05 – Príloha č.2“ je súčasťou bezpečnostných opatrení, ktoré popisujú riadenie vzťahov s tretími stranami v zmysle Zákona. Upravuje spôsob a rozsah povinností tretej strany pri hlásení kybernetického bezpečnostného incidentu Prevádzkovateľovi základnej služby (ďalej PZS). Tretia strana je povinná riadiť sa touto smernicou v zmysle požiadavky §20, odsek 3 písmeno e) Zákona.
Smernica:

a) Definuje pojem KBI
b) Upravuje spôsob hlásenia KBI
c) Určuje rozsah informácií, ktoré hlásenie KBI musí obsahovať
d) Definuje ostaté povinnosti tretej strany súvisiace so vznikom a hlásením KBI

Dokument je zároveň prílohou Zmluvy, ktorú je ZsVS ako Prevádzkovateľ základnej služby povinný v zmysle Zákona, § 19, odstavec 2, pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných technológií ZsVS s treťou stranou ako dodávateľom uzatvoriť.

2. ROZSAH PLATNOSTI

Dokument je platný a záväzný pre každú tretiu stranu, ktorá vykonáva činnosti alebo práce na základe zmluvy o dielo, servisnej zmluvy, zmluvy o poskytovaní služieb alebo inej zmluvy na objektoch IKT v IT alebo OT infraštruktúry ZsVS a pre každého zamestnanca ZsVS, ktorý je poverený sprevádzaním tretej strany, riadením alebo koordinovaním servisných činností tretej strany na IT alebo OT infraštruktúre ZsVS.

3. ZODPOVEDNOSTI A SPOLUPRÁCA

ZsVS zodpovedá za prijatie postupov týkajúcich sa kybernetickej a informačnej bezpečnosti, spracovaných podľa smernice riadenia ISMS dokumentácie a preukázateľné oboznámenie sa všetkých zamestnancov ZsVS s obsahom bezpečnostnej dokumentácie.

MKB vyhodnocuje riziko prístupu tretej strany do infraštruktúry ZsVS, posudzuje rozsah aplikovania zmien na prvkoch infraštruktúry z pohľadu kybernetickej bezpečnosti, vyhodnocuje riziká a incidenty.

Predkladateľ zmluvy s treťou stranou je zodpovedný za komunikáciu s MKB pre posúdenie rozsahu aplikovaných bezpečnostných opatrení pre tretiu stranu a za preukázateľné oboznámenie tretej strany s týmto dokumentom.

Tretia strana je povinná informovať všetkých svojich zamestnancov, ktorí budú realizovať zmluvné zásahy na systémoch a zariadeniach ZsVS o povinnosti dodržiavania bezpečnostných opatrení v zmysle tohto dokumentu

5. POSTUPY HLÁSENIA KBI VOČI PZS

5.1. Vymedzenie pojmu KBI

Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:

- strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
- obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
- vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby,
- ohrozenie bezpečnosti informácií,

5.2. Posúdenie závažnosti KBI

V zmysle **§ 24** Zákona je Prevádzkovateľ základnej služby povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov.
Závažný kybernetický bezpečnostný incident sa v zmysle **§ 24** Zákona člení na kategóriu prvého (I) stupňa, druhého (II) stupňa a tretieho (III) stupňa v závislosti od:
a) počtu používateľov základnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
b) dĺžky trvania kybernetického bezpečnostného incidentu,
c) geografického rozšírenia kybernetického bezpečnostného incidentu,
d) stupňa narušenia fungovania základnej služby alebo digitálnej služby,
e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.

Posúdenie dopadu KBI vzniknutého činnosťou tretej strany na základnú službu ZsVS, ako aj posúdenie dopadu KBI, ktorý vznikne na IKT tretej strany, pričom príslušné prvky IKT tretej strany, na ktorých KBI vznikol, slúžia na poskytovanie servisnej služby pre ZsVS (VPN prepojenie sietí, vzdialený prístup do infraštruktúry ZsVS pre správu prvkov IKT infraštruktúry ZsVS, alebo iné spôsoby pripojenia IKT tretej strany k IKT ZsVS) **rieši MKB ZsVS.**

Tretia strana je povinná hlásiť každý KBI, ktorý spozoruje pri riešení servisnej činnosti, bez ohľadu na jeho závažnosť. Hlásenie realizuje spôsobom a rozsahom popísaným v tomto dokumente.

5.3. Spôsob reakcie na KBI

Tretia strana reaguje na spozorovaný kybernetický bezpečnostný incident nasledovne:
1) Pri vykonávaní servisných prác priamo na mieste v objektoch ZsVS – on-site:
- ak je incident spozorovaný na IKT prostriedku tretej strany (počítač, notebook, smart zariadenie) pripojenom do infraštruktúry IKT ZsVS, zamestnanec tretej strany **okamžite odpojí IKT prostriedok zo siete ZsVS**
- ak je incident spozorovaný na IKT prostriedku ZsVS, okamžite kontaktuje zamestnanca ZsVS, ktorý ho pri servisnej činnosti sprevádza, prípadne, ktorý je za odovzdanie či správnosť realizácie servisného úkonu zodpovedný. Ak nie je dostupný, kontaktuje dostupného pracovníka na Útvare IT alebo Útvare dispečing, ak sa jedná o OT infraštruktúru (ASRT a dispečerské pracoviská) a postupuje podľa pokynov pracovníka ZsVS.
- Následne vyplní hlásenie o KBI, ktoré v písomnej podobe odovzdá pracovníkovi na Útvare IT alebo Útvare dispečing, ak sa jedná o OT infraštruktúru a hneď ako je to možné mailom zašle na kybermanager@zsvs.sk.

2) Pri vykonávaní servisných prác na diaľku – on-line:
- ak je incident spozorovaný na IKT prostriedku tretej strany (počítač, notebook, smart zariadenie) pripojenom on-line do infraštruktúry IKT ZsVS, zamestnanec tretej strany **okamžite odpojí IKT prostriedok zo siete ZsVS**

- ak je incident spozorovaný na IKT prostriedku ZsVS (počítač, server, služba, na ktorej tretia strana vykonáva servisnú činnosť), okamžite kontaktuje dostupného pracovníka na Útvare IT alebo Útvare dispečing, ak sa jedná o OT infraštruktúru (ASRT a dispečerské pracoviská) a postupuje podľa pokynov pracovníka ZsVS.
- Následne vyplní hlásenie o KBI, ktoré mailom zašle na kybermanager@zsvs.sk.

3) Pri vzniku KBI na IKT infraštruktúre tretej strany:

- Pracovník tretej strany informuje o vzniku KBI svojho nadriadeného a postupuje podľa interných smerníc tretej strany na riadenie KBI.
- Ak je to KBI na internej infraštruktúre tretej strany, z ktorej sa realizujú servisné zásahy, alebo KBI na infraštruktúre na ktorej sa vyvíja alebo testuje produkt dodávaný ZsVS, je povinnosť tretej strany okamžite po zistení KBI informovať ZsVS a to vyplnením hlásenia o KBI a zaslaním na mail kybermanager@zsvs.sk.
- Akýkoľvek iný KBI na vlastnej IKT infraštruktúre je tretia strana povinná analyzovať, či nemôže mať sekundárny vplyv na bezpečnosť poskytovaných služieb pre ZsVS, informáciu o KBI a výsledok analýzy vplyvu zaslať mailom na kybermanager@zsvs.sk.

ZsVS a tretia strana si môžu dohodnúť aj iný spôsob hlásenia KBI, musí však platiť, že reakcia na odhalený KBI je okamžitá a aj informovanie príslušného zamestnanca ZsVS je okamžité. Ako ďalšie kanály hlásenia vzniku KBI môžu byť telefonát, SMS, funkčný servisný portál a pod. V takom prípade musí byť mechanizmus hlásenia KBI upravený aj v tomto dokumente.

5.4. Rozsah údajov pri hlásení KBI

Hlásenie kybernetických bezpečnostných incidentov podľa § 24 ods. 4 Zákona musí obsahovať minimálne a najmä informácie (v zmysle § 2 Vyhlášky 165/2018 Z. z.):

a) o tom, kto hlási závažný kybernetický bezpečnostný incident, a to:

- identifikačné údaje tretej strany
- kontaktné údaje tretej strany

b) o kybernetickom bezpečnostnom incidente, a to:

- časové údaje priebehu kybernetického bezpečnostného incidentu,
- detailný opis priebehu kybernetického bezpečnostného incidentu
- rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu

c) o službe, ktorá bola zasiahnutá kybernetickým bezpečnostným incidentom, a to

- konkrétny popis všetkých zasiahnutých aktív
- vplyv kybernetického bezpečnostného incidentu na poskytovanú službu,

d) o riešení závažného kybernetického bezpečnostného incidentu, a to

- ako bol kybernetický bezpečnostný incident riešení okamžite po odhalení
- aké sú navrhnuté a vykonané nápravné opatrenia, aby sa incident neopakoval

- popis následkov kybernetického bezpečnostného incidentu.

Vzor hlásenia KBI – formulár – je v prílohe tohto dokumentu. Na požiadanie môže byť tento vzor hlásenia KBI poskytnutý tretej strane v elektronickej forme .docx alebo .pdf

6. REGISTER SÚVISIACICH DOKUMENTOV

Zmluva
SM_05_P1_Všeobecné požiadavky na fyzickú a informačnú bezpečnosť
Zonácia vodohospodárskych objektov

7. ZMENOVÉ RIADENIE A PLATNOSŤ

Tento dokument nadobúda účinnosť dňom jeho schválenia predstavenstvom ZsVS. Jeho aktualizácia sa vykonáva podľa potreby, revízie sa vykonávajú minimálne 1 x za 2 roky. Zodpovednosť za zmeny a právo kontroly dodržovania ustanovení tejto smernice má MKB. Doba platnosti nie je obmedzená.

8. ZOZNAM PRÍLOH

Formulár – Hlásenie KBI

HLÁSENIE KYBERNETICKÉHO BEZPEČNOSTNÉHO INCIDENTU (KBI)

Identifikačné a kontaktné údaje tretej strany:

Názov a IČO spoločnosti: .....

Meno, Priezvisko osoby, ktorá hlási incident .....

Pracovná pozícia osoby, ktorá hlási incident .....

Popis KBI:

Dátum a čas spozorovania KBI: .....

Typ KBI (čo bolo spozorované): .....

Popíšte slovne, alebo vyberte: .....

- o Nežiadúci obsah (SPAM, Phishing)
- o Prejav škodlivého kódu (vírus, malvér, ransomvare, ...)
- o Získavanie informácií (skenovanie siete, odpočúvanie, sociálne inžinierstvo, ...)
- o Pokus o prienik do systému alebo siete
- o Podozrenie na úspešný prienik do systému alebo siete
- o Nedostupnosť prostriedkov spôsobená útokom (DoS, DDoS, sabotáž, výpadok služby)
- o Neoprávnený prístup k informáciám (zneužitie účtu, útok na heslá)
- o Únik informácií (kopírovanie, alebo iný prenos informácií neoprávnenou cestou)
- o Poškodenie informácií (úmyselné alebo neúmyselné chybou technológie)
- o Podvodné konanie (zneužitie autorizácie, neoprávnené využívanie IKT, porušenie autorských práv)
- o Zistenie zraniteľnosti na IKT
- o Iné – potrebné písomne uviesť vyššie

Zasiahnuté služby a/alebo aktíva:

Ktoré aktíva (zariadenia, siete, služby, aplikácie) boli zasiahnuté (uveďte podrobne)

.....

.....

Vplyv KBI na aktívum:

- o zastavenie prevádzky, nedostupnosť aktíva (uveďte dobu nedostupnosti v hodinách) .....
- o obmedzenie prevádzky, zníženie výkonnosti (uveďte % od .....
- o ohrozenie, obmedzenie prevádzky iného aktíva (uveďte akého) .....
- o iné: .....

Postup pri riešení KBI:

Okamžité opatrenia. .....

Preventívne opatrenia (návrh opatrení na zabránenie opakovania KIB) .....

.....

.....

.....

Odhadované následky KIB: .....

.....

.....