ZMLUVA

o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatvorená medzi

Objednávateľ

Obchodné meno:	**Zvolenská teplárenská, a.s.**
Sídlo:	Lučenecká cesta 25, 961 50 Zvolen
IČO:	36052248
Zápis v registri:	v Obchodnom registri Okresného súdu Banská Bystrica, Oddiel Sa, vložka č. 686/S
Za ktorú koná:	Ing. Anton Brčka – predseda predstavenstva, a.s. Ing. Norbert Skákala – člen predstavenstva, a.s.
Kontaktný mail:	
Oprávnený zamestnanec:	Ing. Róbert Mramúch, manažér kybernetickej bezpečnosti

(ďalej aj ako „**Objednávateľ**“ alebo „**Prevádzkovateľ základnej služby**“)

a

Dodávateľ

Obchodné meno:	**PMG agency, s.r.o**
Sídlo:	Jilemnického 22, 031 01 Liptovský Mikuláš, Slovenská republika
IČO:	44 192 568
DIČ:	2022622250
IČ DPH:	SK2022622250
Zápis v registri:	v Obchodnom registri Okresného súdu Žilina, Oddiel: Sro, vložka č.20657/L
Za ktorú koná:	Milan Droppa – konateľ spoločnosti

(ďalej aj ako „**Dodávateľ**“ alebo „**Tretia strana**““)

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

vzhľadom k tomu, že

- spoločnosť **Zvolenská teplárenská, a.s.** je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o kybernetickej bezpečnosti**“ alebo „**ZoKB**“),

- základnou službou prevádzkovateľa základnej služby je výroba tepla, dodávka tepla a výroba elektriny,

- dodávateľ uzatvoril s prevádzkovateľom základnej služby predbežnú objednávku ktorej predmet priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v zákone o kybernetickej bezpečnosti, pre prevádzkovateľa základnej služby,

- prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti (ďalej ako „**ZoBOaNP**"),

- táto ZoBOaNP ustanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov PZS počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov PZS, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany prevádzkovateľa základnej služby (ďalej len „**ciele**"), a to v spolupráci s dodávateľom,

- plnenie povinností podľa tejto ZoBOaNP sa vyžaduje počas celej doby trvania zmluvy,

takto:

1. PREDMET DOHODY

1.1 Pojmy používané v tejto ZoBOaNP majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

1.2 Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, minimálne v rozsahu uvedenom v tejto ZoBOaNP tak, aby boli naplnené ciele tejto ZoBOaNP. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami podľa ZoBOaNP.

1.3 Dodávateľ je zároveň povinný dodržiavať bezpečnostné smernice prevádzkovateľa základnej služby, s ktorými ho PZS písomne oboznámi. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými smernicami prevádzkovateľa základnej služby.

1.4 Dodávateľ berie na vedomie, že bezpečnostné opatrenia deklarované v podobe bezpečnostných smerníc, sa môžu počas doby trvania zmluvy meniť tak, aby reagovali na novo-identifikované kybernetické hrozby pre dodávaný systém alebo službu. Dodávateľ bude na takéto zmeny v bezpečnostných smerniciach a štandardoch upozornený a dohodne sa s PZS na podmienkach nasadenia potrebných bezpečnostných opatrení, ktoré je v jeho silách zabezpečiť v primeranej kvalite, cene a čase.

1.5 Dodávateľ je povinný plniť notifikačné povinnosti podľa požiadaviek ZoKB tak, aby boli naplnené ciele tejto ZoBOaNP.

1.6 Dodávateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z požiadaviek ZoKB, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek ZoKB.

1.7 Plnenie povinností podľa tejto ZoBOaNP tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa základnej služby podľa zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto ZoBOaNP po celú dobu trvania zmluvy.

1.8 Odplata za plnenie povinností dodávateľa podľa tejto ZoBOaNP a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto ZoBOaNP sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom základnej služby dodávateľovi podľa zmluvy a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto ZoBOaNP od prevádzkovateľa základnej služby nemá nárok.

2. ZÁKLADNÉ POŽIADAVKY NA KYBERNETICKÚ BEZPEČNOSŤ PRE DODÁVATEĽA

Dodávateľ má:

2.1 povinnosť dodržiavať interné bezpečnostné predpisy PZS, s ktorými bude oboznámený buď pred podpisom zmluvy (viď Príloha č. 3 Všeobecné bezpečnostné požiadavky na dodávaný ICT produkt alebo službu) alebo po jej podpísaní a to podľa povahy dodávaného diela alebo prác (viď Príloha č. 4 Ostatné bezpečnostné smernice alebo štandardy kybernetickej bezpečnosti PSZ),

2.2 povinnosť zabezpečiť, aby akékoľvek zásahy alebo zmeny v produkte alebo službe počas ich nasadzovania, prevádzky a technickej podpory vykonávali len dodávateľom autorizované, odborne zdatné a na základy informačnej a kybernetickej bezpečnosti poučené osoby,

2.3 vyžiadať si súhlas PZS na prípadné využitie tretích strán ako subdodávateľov,

2.4 za základné bezpečnostné požiadavky sa považujú predovšetkým také, ktoré sú aplikovateľné bez ohľadu na typ produktu alebo služby. Nasledovné základné bezpečnostné požiadavky sú povinné a dodávateľ sa zaväzuje ich plniť počas celej doby trvania zmluvy,

2.5 dodávateľ poskytuje aktuálny zoznam všetkých komponentov použitých v riešení na úrovní výrobcov a verzií,

2.6 produkt/služba sú dodávané vo výrobcom alebo výrobcami jednotlivých komponentov podporovaných verziách,

2.7 dodávateľ včas upozorňuje PZS na zistené bezpečnostné (technické) zraniteľnosti dodávaného produktu/služby, vrátane všetkých komponentov, ktoré zistil sám alebo o ktorých sa dozvedel,

2.8 dodávaný produkt/služba je pravidelne aktualizovaný na bezpečnostné záplaty – buď priamo dodávateľom alebo nepriamo prostredníctvom aktualizovaných návodov od dodávateľa,

2.9 dodávateľ upozorňuje PZS na všetky udalosti, zmeny v ním dodávanom produkte/službe, ktoré môžu alebo mohli viesť k bezpečnostnému incidentu (nesprávna konfigurácia, neoprávnený alebo pokus o neoprávnený prístup, zneužitie prístupov oprávnenou osobou, chýbajúce bezpečnostné záplaty, výsledok scanu na technické zraniteľnosti a pod.),

2.10 dodávateľ dodáva produkt alebo službu v minimálne nevyhnutnej a zabezpečenej konfigurácii.

3. PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

Pre účely tohto dokumentu sa za bezpečnostný incident považuje udalosť, ktorá reálne alebo potenciálne ohrozila dôvernosť, integritu alebo dostupnosť informačných aktív, priamo alebo nepriamo súvisiacich s poskytovaním základných služieb v zmysle ZoKB.

3.1 Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby

alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby, (ďalej len „**incidenty**"):

a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa základnej služby,
b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy a tejto ZoBOaNP, alebo budú mať prístup k informáciám prevádzkovateľa základnej služby,
c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
d) sledovať hrozby dotýkajúce sa dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,
e) predchádzať vzniku incidentov,
f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o bezpečnostných incidentoch,
g) prijímať od prevádzkovateľa základnej služby varovania pred bezpečnostnými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,
h) zasielať prevádzkovateľovi základnej služby včasné varovania pred bezpečnostnými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto ZoBOaNP alebo inak, a
i) spolupracovať s prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.

3.2 Dodávateľ je povinný počas trvania tejto ZoBOaNP mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto ZoBOaNP a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto ZoBOaNP.

3.3 Dodávateľ je povinný doručiť prevádzkovateľovi základnej služby zoznam pracovných rolí dodávateľa, ako aj úplný zoznam svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy a tejto ZoBOaNP alebo budú mať prístup k informáciám prevádzkovateľa základnej služby, ktorý sa jeho doručením prevádzkovateľovi základnej služby stane súčasťou tejto ZoBOaNP, v min. rozsahu podľa Prílohy č. 1.

3.4 Dodávateľ je povinný doručiť prevádzkovateľovi úplný zoznam svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy a tejto ZoBOaNP, alebo budú mať prístup k informáciám prevádzkovateľa základnej služby, a každú zmenu v personálnom obsadení je dodávateľ povinný prevádzkovateľovi základnej služby písomne oznámiť, pričom pre oznamovanie zmien sa použijú ustanovenia zmluvy o doručovaní.

3.5 Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto ZoBOaNP v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi základnej služby na nahliadnutie a zhotovenie kópií.

3.6 Dodávateľ je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN ISO/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) min. v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa základnej služby.

3.7 Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, 10, 12, 14 a 15 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, a v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa základnej služby.

4. REAKTIVITA PRI RIEŠENÍ INCIDENTOV

4.1 Dodávateľ je povinný bezodkladne hlásiť každý incident prevádzkovateľovi základnej služby spôsobom určeným prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, dodávateľ je povinný odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

4.2 Dodávateľ je povinný riešiť incidenty najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len „**reaktívne opatrenie**"). Pri riešení incidentov je dodávateľ povinný na žiadosť prevádzkovateľa základnej služby spolupracovať s prevádzkovateľom základnej služby, Národným bezpečnostným úradom a Ministerstvom hospodárstva Slovenskej republiky, prípadne ďalšími orgánmi verejnej správy a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto ZoBOaNP alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.

4.3 Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní, a poskytnúť ho prevádzkovateľovi základnej služby.

4.4 Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.

4.5 Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.

4.6 Po vyriešení incidentu je dodávateľ na výzvu prevádzkovateľa základnej služby v určenej lehote povinný predložiť prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „**bezpečnostné opatrenia**") na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom základnej služby na jeho návrhu.

4.7 Po schválení bezpečnostného opatrenia prevádzkovateľom základnej služby, je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať.

4.8 Po vykonaní bezpečnostného opatrenia dodávateľom, je dodávateľ povinný preveriť jeho účinnosť.

5. MLČANLIVOSŤ

5.1 Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy a tejto ZoBOaNP, ktoré nie sú verejne známe a ktoré by mohli uľahčiť kybernetický útok, alebo viesť ku kybernetickému incidentu (najmä informácie o IT/OT architektúre, používaných systémoch, ich dodávateľoch a verziách, o topológii sietí, o konfiguráciách a pod.).

5.2 V prípade pochybností o tom, ktoré z takýchto informácií sa týkajú kybernetickej bezpečnosti, platí pre dodávateľa pravidlo, že všetky informácie súvisia s kybernetickou bezpečnosť, a preto musí o nich zachovávať mlčanlivosť.

5.3 Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto ZoBOaNP.

5.4 Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.

5.5 Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu alebo obchodného vzťahu.

5.6 Po ukončení tejto ZoBOaNP, je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto ZoBOaNP prístup, resp. tieto podľa pokynu prevádzkovateľa základnej služby zničiť.

6. KONTAKTNÉ OSOBY PRE OBLASŤ KYBERNETICKEJ BEZPEČNOSTI

6.1 Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto ZoBOaNP s prevádzkovateľom základnej služby spôsobom určeným prevádzkovateľom základnej služby, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

6.2 Prevádzkovateľ základnej služby určuje nasledovnú kontaktnú osobu pre komunikáciu s dodávateľom pre oblasť kybernetickej bezpečnosti:
Ing. Róbert Mramúch, [redacted]

6.3 Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s prevádzkovateľom základnej služby pre oblasť kybernetickej bezpečnosti:
Meno a priezvisko:
Tel:
Email:

6.4 Kontaktné osoby podľa odsekov 6.2 alebo 6.3 tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia zmluvy o doručovaní.

7. SPOLOČNÉ USTANOVENIA

7.1 Dodávateľ je povinný plniť povinnosti podľa tejto ZoBOaNP, v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

7.2 Dodávateľ je ďalej povinný plniť povinnosti podľa tejto ZoBOaNP v súlade so sektorovými bezpečnostnými opatreniami, ktoré vydáva Ministerstvo hospodárstva Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.

7.3 Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

7.4 Dodávateľ je povinný mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto ZoBOaNP, v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.

7.5 Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto ZoBOaNP (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa základnej služby, mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.

7.6 Dodávateľ je povinný plniť povinnosti podľa tejto ZoBOaNP bezodkladne.

7.7 V prípade, ak dodávateľ plní zmluvu prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, je povinný zabezpečiť plnenie povinností vyplývajúcich z tejto ZoBOaNP aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto ZoBOaNP. Dodávateľ je povinný zabezpečiť, aby prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto ZoBOaNP aj u týchto subdodávateľov.

7.8 Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto ZoBOaNP ohrozuje plnenie cieľov tejto ZoBOaNP, pričom za dôsledky incidentov, ktoré by sa pri riadnom a včasnom plnení povinností dodávateľa podľa tejto ZoBOaNP neprejavili, alebo by sa prejavili v menšej intenzite, zodpovedá prevádzkovateľovi základnej služby v plnom rozsahu (zodpovednosť za výsledok).

8. AUDIT KYBERNETICKEJ BEZPEČNOSTI

8.1 Prevádzkovateľ základnej služby je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto ZoBOaNP a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov tejto ZoBOaNP.

8.2 Prípadné nedostatky zistené auditom, je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.

8.3 Prevádzkovateľ základnej služby môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti PZS pri výkone auditu realizuje prevádzkovateľom základnej služby poverená tretia osoba.

8.4 Dodávateľ je povinný pri audite spolupracovať s PZS a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh podľa tejto ZoBOaNP.

8.5 Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh podľa tejto ZoBOaNP.

8.6 V rámci auditu je dodávateľ povinný preukázať PZS súlad s touto ZoBOaNP, najmä preukázať svoju pripravenosť plniť úlohy podľa tejto ZoBOaNP, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov

a ich zamestnancov o povinnosti mlčanlivosti podľa tejto ZoBOaNP a aktuálnosť svojej bezpečnostnej dokumentácie.

8.7 Prevádzkovateľ základnej služby je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer realizovať u dodávateľa audit.

8.8 Vykonanie alebo nevykonanie auditu prevádzkovateľom základnej služby nezbavuje dodávateľa zodpovednosti za plnenie povinností dodávateľa vyplývajúcich z tejto ZoBOaNP.

8.9 Dodávateľ je povinný písomne informovať PZS o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom.

8.10 Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy podľa tejto ZoBOaNP.

8.11 Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Ustanovenia článku 5 ods. 5.3 a 5.4 tejto ZoBOaNP platia rovnako a ustanovenie článku 5 ods. 5.5 tejto ZoBOaNP platí primerane.

8.12 Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne dodávateľ. Dodávateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch dodávateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory dodávateľa.

9. SANKCIE

9.1 Zmluvná strana zodpovedá za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinnosti zmluvnej strany stanovenej zákonom o kybernetickej bezpečnosti alebo ZoBOaNP.

9.2 V prípade, že zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo zákona o kybernetickej bezpečnosti alebo ZoBOaNP (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.

9.3 V prípade preukázateľnej existencie príčinnej súvislosti podľa tohto článku 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 ZoBOaNP, alebo na inú porušujúcou zmluvnou stranou oznámenú adresu.

9.4 Dodávateľ berie na vedomie, že nesplnenie akejkoľvek jeho povinnosti podľa tejto ZoBOaNP môže ohroziť plnenie cieľov tejto ZoBOaNP, pričom za dôsledky incidentov, ktoré by sa pri riadnom a včasnom plnení povinností dodávateľom podľa tejto ZoBOaNP neprejavili, alebo by sa prejavili v menšej intenzite, zodpovedá prevádzkovateľovi základnej služby v plnom rozsahu (zodpovednosť za výsledok) a zároveň sa zaväzuje zaplatiť na základe uplatnenia Prevádzkovateľom základnej služby za každé takéto porušenie zmluvnú pokutu vo výške 5000,- eur. Dodávateľ je povinný odstrániť akékoľvek porušenie povinností podľa tejto ZoBOaNP

bezodkladne po oznámení prevádzkovateľa základnej služby, najneskôr však do 3 dní od jeho vzniku, ak sa zmluvné strany nedohodnú písomne inak, pričom porušenie tohto ustanovenia ZoBOaNP bude považované za jej podstatné porušenie, s právom prevádzkovateľa základnej služby od ZoBOaNP odstúpiť, pričom povinnosť nahradiť vzniknutú škodu ostáva zachovaná v celom rozsahu.

9.5 V prípade, že v dôsledku porušenia povinností vyplývajúcich z tejto zmluvy dodávateľom vznikne PZS povinnosť hradiť poplatky, pokuty alebo iné peňažné sankcie, uplatnené orgánmi verejnej správy voči PZS, je dodávateľ povinný nahradiť PZS vyššie uvedené sankcie

10. ZÁVEREČNÉ USTANOVENIA

10.1 Táto ZoBOaNP sa uzatvára na dobu určitú do doby platnosti hlavnej zmluvy. PZS je oprávnený od tejto ZoBOaNP odstúpiť v prípadoch, ak dodávateľ porušuje svoje povinnosti vyplývajúce z tejto ZoBOaNP. Odstúpenie od tejto ZoBOaNP sa musí urobiť písomne, inak sa na neho neprihliada. Pre doručovanie odstúpenia od tejto ZoBOaNP sa použijú ustanovenia zmluvy o doručovaní. Zrušenie tejto ZoBOaNP sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zrušení tejto ZoBOaNP, a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto ZoBOaNP, ku ktorému dôjde do zrušenia tejto ZoBOaNP.

10.2 Po ukončení tejto ZoBOaNP je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na PZS všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto ZoBOaNP.

10.3 Táto ZoBOaNP sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy neupravené touto ZoBOaNP sa riadia ustanoveniami Obchodného zákonníka č. 513/1991 Zb. v znení neskorších predpisov a súvisiacimi predpismi.

10.4 Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov týkajúcich sa tejto ZoBOaNP. V prípade, ak dodávateľom bude zahraničná osoba, zmluvné strany sa dohodli, že miestne príslušným súdom bude súd, v obvode ktorého má sídlo PZS.

10.5 Táto ZoBOaNP sa môže meniť alebo ukončiť iba dohodou zmluvných strán v písomnej forme.

10.6 Ak by sa dôvod neplatnosti vzťahoval len na časť tejto ZoBOaNP, bude neplatnou len táto časť.

10.7 Táto ZoBOaNP tvorí úplnú dohodu medzi zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto ZoBOaNP zanikajú všetky predchádzajúce písomné a ústne dohody súvisiace s predmetom tejto ZoBOaNP a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych v tejto ZoBOaNP neuvedených ústnych dojednaní a dohôd.

10.8 Táto ZoBOaNP bola vyhotovená v dvoch rovnopisoch, po jednej pre každú zmluvnú stranu.

10.9 Zmluvné strany berú na vedomie, že PZS je v zmysle § 2 ods. 3 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov povinnou osobou, a preto je táto ZoBOaNP v zmysle § 5a zákona o slobode informácií v spojení s § 47a Občianskeho zákonníka č. 40/1964 Zb. v znení neskorších predpisov povinne zverejňovanou zmluvou.

10.10 Zmluvné strany berú na vedomie, že účinnosť tejto ZoBOaNP je v zmysle § 47a Občianskeho zákonníka v nadväznosti na § 5a zákona o slobode informácií podmienená jej zverejnením v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.

10.11 Táto ZoBOaNP nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv. Súčasťou zverejnenia je aj zoznam pracovných rolí dodávateľa podľa článku 3 ods. 3.3 tejto ZoBOaNP.

10.12 Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto ZoBOaNP neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah ZoBOaNP dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.

V mene prevádzkovateľa základnej služby:

Vo Zvolene, dňa .....

Objednávateľ:

[redacted]

Ing. Anton Brčka – predseda predstavenstva

[redacted]

Ing. Norbert Skákala – člen predstavenstva

V mene dodávateľa:

V Liptovskom Mikuláši, dňa 2. marca 2022

Dodávateľ:

Milan Droppa – konateľ spoločnosti

[redacted]

Príloha č. 1 - Zoznam pracovných rolí dodávateľa a ich personálne obsadenie:

Meno pracovníka	Pracovná rola	Spoločnosť
Milan Droppa	Konateľ spoločnosti / dátový analytik	PMG agency, s.r.o.
Ing. Milan Jančuška	Dátový špecialista - programátor	PMG agency, s.r.o.

Príloha č. 2 Požiadavky na kybernetickú bezpečnosť dodávaného produktu alebo služby typu COTS

1. Aplikovateľnosť

Táto príloha slúži ako vzor bezpečnostných požiadaviek na dodávateľa komerčného produktu alebo služby, teda takých, ktoré nie sú z pohľadu nasadenia do prevádzky pre zákazníka (PZS) nijako špeciálne upravované, alebo vyrábané na mieru (napr. štandardný produkt typu CMS, riadiaci systém, dochádzkový systém apod.) a dodávajú sa ako hotové produkty (COTS - Commercial Off-The Shelf).

2. Skupiny požiadaviek na kybernetickú bezpečnosť

V podmienkach organizácie existujú dve skupiny požiadaviek na kybernetickú bezpečnosť: základné a rozšírené.

Prvá skupina predstavuje **povinné** požiadavky, ktoré sú uvedené v dokumente **ZMLUVA o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov**.

Druhá skupina obsahuje **voliteľné** požiadavky, ktoré sa volia podľa bezpečnostného profilu produktu alebo služby, teda podľa možných kybernetických hrozieb pre organizáciu. Dodávateľ sa vyjadruje ku všetkým oblastiam týchto požiadaviek tak, aby bolo možné spätne preukázať, ktoré z nich boli akceptované.

Všetky povinné a rozšírené požiadavky na kybernetickú bezpečnosť, ktoré sa dodávateľ zaviaže splniť, budú PZS overené minimálne prvý krát – pri akceptácii produktu alebo služby pred uvedením do prevádzky a potom kedykoľvek priebežne, náhodne, alebo pri každej významnej zmene, napr. pri aktualizácii alebo upgrade na vyššiu, alebo inak rozšírenú verziu produktu alebo služby.

3. Rozšírené požiadavky na kybernetickú bezpečnosť

Tieto požiadavky sú voliteľné a vyplývajú z charakteru používania produktu alebo služby. Dodávateľ je povinný označiť požiadavky, ktoré sú z pohľadu jeho vlastnej zodpovednosti nerelevantné (lebo ich nemôže ovplyvniť) a tie, ktoré sa zaväzuje splniť (lebo ich priamo ovplyvňuje) a ktoré aj budú predmetom kontroly skutočného stavu zo strany PZS.

Za priame ovplyvnenie bezpečnosti produktu a jeho komponentov dodávateľom, sa považuje hlavne:

- výber komponentov dodávaného riešenia, ako sú operačné systémy, databázy, web servery, systémové alebo aplikačné knižnice, protokoly a i. (nesmie ísť o zastarané, nepodporované, nezabezpečené, nezaplátané verzie)
- pred-definovaná a nezabezpečená konfigurácia (default účty, služby, porty, knižnice, vzorové dáta, šablóny, jazyková podpora apod.)
- Medzi rozšírené požiadavky patria požiadavky v týchto oblastiach oblastiach:
- operačný systém, sieť a sieťové konfigurácie, databáza, aplikácia vrátane web rozhraní a ich komponentov, bezpečnosť dát (dôvernosť, integrita, dostupnosť), riadenie zraniteľností, nasadzovanie záplat a bezpečná konfigurácia (hardening).

3.1 Systémová bezpečnosť

3.1.1 Bezpečná počiatočná konfigurácia (secure zero configuration)

Systémy, na ktorých sa prevádzkuje daný produkt alebo služba, vrátane súvisiacich systémových služieb, knižníc, databáz alebo nevyhnutných aplikácií, sú dodané v bezpečnej konfigurácii a v najaktuálnejších, výrobcami podporovaných, stabilných verziách a s bezpečnostnými záplatami, ktoré boli v čase dodávky k dispozícii.

Na systéme nie sú ponechané prípadné pred-definované (default) účty, všeobecné nastavenia v konfiguráciách a všetky nepotrebné/nevyužívané komponenty alebo systémové služby sú odstránené.

Dodávateľ poskytne zoznam všetkých dodávaných kompomentov produktu alebo služby, potvrdí ich bezpečnú konfiguráciu, nasadenie najnovších bezpečnostných záplat a zaručí, že ide o verzie podporované príslušnými výrobcami.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.1.2 Účty a autentifikácia

Dodávateľ prehlasuje, že dodaný produkt alebo služba používa na úrovni systému len také účty (personálne, technické, servisné), ktoré sú nevyhnutné pre ich správne používanie a prevádzku, aplikuje na ne princíp minimálne nevyhnutných práv a privilégií, princíp oddeľovania rolí a používa iba bezpečné autentizačné metódy, protokoly a algoritmy, ktoré zaručujú dôvernosť autentizačných prvkov (šifrovanie hesiel počas prenosu aj uloženia, viac-faktorová autentizácia apod.) a nezneužiteľnosť identity, ktorú predstavujú.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.1.3 Súborový systém

Dodávaný produkt alebo služba zaručuje striktné oddelenie aplikačnej vrstvy od nižších vrstiev ako sú databáza, web server a operačný systém tak, aby k nim koncový používateľ produktu alebo služby nemal možnosť priameho prístupu, ak to nie je nevyhnutné pre ich správne fungovanie.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.1.4 Konfigurované systémové služby

Dodávaný produkt alebo služba sú nakonfigurované s minimálnym footprintom, to znamená, že obsahujú len tie systémové služby, knižnice a systémové nástroje (kompilátory, interpretery, debuggery), ktoré sú na ich prevádzku nevyhnutné.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.2. Antimalvérová ochrana

Na všetkých komponentoch produktu alebo služby, ktoré môžu prísť do styku s nedôveryhodným prostredím, ako je internet alebo koncový používateľ, ktorý napr. môže ukladať alebo spúšťať aktívny kód, program alebo skript, musí byť umožnené inštalovať antimalvérovú ochranu, ktorá je riadená z centrálneho miesta.

Ak nie je možné, z funkčných alebo prevádzkových dôvodov, nasadenie antimalvérového produktu (agenta monitorujúceho v reálnom čase) priamo na dodávaný systém alebo službu, musí dodávateľ definovať aspoň podmienky, za akých je možné rizikové miesta (napr. na ukladanie súborov) pravidelne scanovať na škodlivý kód.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.3 Sieťová bezpečnosť

3.3.1 Segregácia sietí

Architektúra dodávaného produktu alebo služby musí zaručiť ich kontrolované oddelenie od nedôveryhodného prostredia (vnútorného alebo externého) prostredníctvom firewallov, ACL, VPN alebo VLAN technológií tak, aby s nimi mohli komunikovať len autorizované strany.

Systémy hostujúce prevádzkovaný produkt alebo službu majú povolené iba nevyhnutné služby a porty a všade tam, kde je to technicky možné, sa uprednostňujú neprivilegované porty (>1024).

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.3.2 Nezabezpečené protokoly

Dodávaný produkt alebo služba nepoužíva nezabezpečené (clear-text) protokoly (napr. ftp, telnet, rlogin) na také aktivity, ktorými je ohrozená dôvernosť alebo integrita prenášaných dát, teda najmä pri komunikácii cez nedôveryhodné prostredia, interné alebo externé.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.3.3 Vzdialené prístupy

Vzdialené prístupy sú povolené iba v prevádzkovo alebo servisne nevyhnutných a odôvodnených prípadoch, nikdy nie priamo na produkčný systém ale na dedikovaný a monitorovaný systém (jump server), pri dodržaní požiadaviek na bezpečnosť, medzi ktoré patrí:

- používanie šifrovaných protokolov (SSL/TLS, ssh apod.),
- obmedzenie prístupu podľa zdrojových adries,
- zaručená identita komunikujúcich strán (najvhodnejšie cez klientský certifikát vydaný PZS),
- protokolárne zachytenie každého vzdialeného pripojenia do žurnálov (log).

Podrobnosti sú v smernici Vzdialený prístup k informačným zdrojom pre tretie strany, ktorá obsahuje požiadavky z najlepšej známej bezpečnostnej praxe.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.3.4 Systémy na detekciu prieniku (IDS) a lokálne firewally

Produkt alebo služba môže byť vybavená alebo doplnená o lokálny (host-based) systém IDS alebo lokálny fireWall.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.4 Kryptografická ochrana a protokoly

Produkt alebo služba používa len také protokoly alebo algoritmy na kryptografickú ochranu (symetrické/asymetrické šifrovanie, hashovacie funkcie), ktoré sú v čase podpísania zmluvy s dodávateľom a za súčasného stavu technológií považované za bezpečné (TLSv1.2, SHA-2/3, SSHv2, SMBv2/3, LLMNR namiesto DNS, Kerberos namiesto NTLMv1 apod).

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.5. Aplikačná bezpečnosť

3.5.1 Účty

Dodávaný produkt alebo služba používa na úrovni aplikácie (databáza, web server, web aplikácia, samostatná aplikácia) len také účty (personálne, technické, servisné), ktoré sú nevyhnutné pre ich správne používanie a prevádzku, aplikuje na ne princíp minimálne nevyhnutných práv a privilégií, princíp oddeľovania rolí a používa iba bezpečné autentizačné metódy, protokoly a algoritmy, ktoré zaručujú dôvernosť autentizačných prvkov (šifrovanie hesiel počas prenosu aj uloženia, viac-faktorová autentizácia apod.) a nezneužiteľnosť identity, ktorú predstavujú.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.5.2 Integrovateľnosť s centrálnou správou účtov

Dodávaný produkt alebo služba umožňuje integráciu s centrálnou správou účtov (IAM, AD/ADFS) organizácie.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.5.3 Riadenie prístupu na základe rolí, skupín alebo federovanej identity

Dodávaný produkt alebo služba umožňuje riadenie práv používateľov využívajúc skupiny používateľov, alebo ich role v systéme alebo organizácii (RBAC), alebo ich claim-based identít (federovaná identita).

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.6 Minimálnosť aplikačného alebo systémového kódu

Dodávaný produkt alebo služba používa len dáta a dátové sety nevyhnutné pre svoju funkcionalitu a teda neobsahuje žiadne nepotrebné demo alebo testovacie dáta, knižnice, pluginy ani lokalizované verzie obsahu v iných jazykoch.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.7 Zaručenie integrity dát

Produkt alebo služba má zavedené mechanizmy na ochranu integrity prenášaných dát a autenticity a identity jej vlastných komunikujúcich systémov a komponentov tak, aby riadiace správy kritické pre prevádzku základných služieb boli chránené proti ich sfalšovaniu a/alebo preposlaniu.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.8. Riadenie verzií, zmien a konfigurácií

Produkt alebo služba obsahuje buď vlastný systém na riadenie verzií, zmien alebo konfigurácií ich komponentov alebo umožňuje integráciu s existujúcim centrálnym riešením v organizácii.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.9. Zaškolenie na bezpečné používanie

Produkt alebo služba sú dodávané aj s dokumentáciou alebo školením na ich bezpečné používanie z pohľadu rizík kybernetickej bezpečnosti.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.10 Bezpečné zlyhanie

Fatálne zlyhanie produktu alebo služby nesmie mať za následok kompletné narušenie atribútov dôvernosti, integrity alebo dostupnosti, teda úplné zlyhanie kybernetickej bezpečnosti.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.11 Žurnálovanie a auditná stopa o bezpečnostných udalostiach

Príkladmi bezpečnostných udalostí: úspešné a neúspešné prihlásenie, zmena v právach a privilégiách, prístup na alebo editovanie objektov v informačnom systéme, zmeny v konfiguráciách, zmeny identifikačných, autentifikačných a autorizačných prvkov atď.

3.11.1 Lokálne žurnálovanie - zaznamenávanie činností používateľov

Dodávaný produkt alebo služba umožňuje jednoznačne identifikovať a preukázať vykonanie kritické alebo citlivé aktivít svojich používateľov (viď príklady bezpečnostných udalostí vyššie). Patria sem aj všetky činnosti privilegovaných používateľov (alebo servisných účtov).

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

Dodávaný produkt alebo služba zaznamenáva lokálne všetky činnosti privilegovaných používateľov (alebo servisných účtov) a vybrané aktivity koncových používateľov.

3.11.2 Vzdialené žurnálovanie

Dodávaný produkt alebo služba umožňuje posielať lokálne vznikajúce záznamy o aktivitách účtov na vzdialené, štandardné systémy na zber a vyhodnocovanie incidentov (SEM alebo SIEM). Udalosti

sú poskytované v štandardných formátoch (napr. json, xml, evtx) a cez štandardné protokoly (napr. rsyslog, WMI/DCOM, MSRPC).

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.11.3 Bezpečnostné incidenty a alarmy

Dodávaný produkt alebo služba obsahujú mechanizmy na automatickú detekciu prevádzkových (kapacita, výkonnosť, úplnosť transakcií apod.) a bezpečnostných incidentov (neoprávnený prístup, zmena v právach a privilégiách, zmena v konfigurácii apod.).

Dodávaný produkt alebo služba má zdokumentovaný proces identifikácie a reakcie na prevádzkové a bezpečnostné incidenty.

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

3.11.4 Zálohovanie a obnova

Dodávaný produkt alebo služba obsahujú mechanizmy a dokumentovaný proces na automatické zálohovanie, kontrolu integrity záloh a bezpečné obnovovanie (dát, systému, komponentov).

☐ požiadavka neaplikovateľná/irelevantná	záväzok dodávateľa splniť požiadavku
vysvetlenie dodávateľa k neaplikovateľnosti požiadavky	
vysvetlenie dodávateľa k prípadnej nesplniteľnosti požiadavky alebo jej časti	

Príloha č. 3 - Všeobecné bezpečnostné požiadavky na dodávaný ICT produkt alebo službu (excerpt z internej smernice)

a) Zodpovednosti tretích strán za kybernetickú bezpečnosť

Základným princípom, ktorý musí každý dodávateľ vziať na vedomie a akceptovať, je jeho zodpovednosť za bezpečnosť ním dodávaného produktu alebo služby do tej miery, aby tieto pre organizáciu nepredstavovali riziko z pohľadu dostupnosti, integrity a dôvernosti jednak pre seba samotné, jednak pre ostatné systémy alebo vnútorné prostredie organizácie, v ktorých musia koexistovať.

Každá **tretia strana** (výrobca, predajca alebo dodávateľ), ktorá poskytuje organizácii produkty alebo služby, pri ktorých dochádza k inštalácii, integrácii, prevádzke, údržbe alebo podpore informačno-komunikačných technológií musí preukázať, do akej miery ich zabezpečila z pohľadu základných atribútov kybernetickej bezpečnosti: dôvernosti, integrity, dostupnosti a nepopierateľnosti (auditovateľnosti).

Keďže informačnú bezpečnosť je možné považovať za integrálnu **súčasť kvality** produktu alebo službu, nesplnenie základných požiadaviek na bezpečnosť môže byť dôvodom pre:

- vo fáze výberu produktu alebo služby - vylúčenie dodávateľa z výberového konania,
- vo fáze preberania - neakceptovanie produktu alebo služby,
- vo fáze prevádzky - uplatnenie sankcií voči dodávateľovi v zmysle podmienok platnej zmluvy.

Dodávateľ musí vedieť organizácii demonštrovať, že architektúra, dizajn, konfigurácia a prevádzka produktu alebo služby zohľadňujú bezpečnostné požiadavky organizácie, ktoré sú definované v tomto dokumente.

V prípade, že dodávateľ vie poskytnúť iné dôkazy o súlade svojho produktu alebo služby s požiadavkami najlepšej známej praxe pre informačnú bezpečnosť (ISO štandardy, štandardy priemyselného odvetvia a pod), organizácia sa môže rozhodnúť ich akceptovať a použiť bezpečnostné požiadavky v nich uvedené do príloh finálnej zmluvy.

Čím menej z týchto požiadaviek sa dodávateľ zaviaže splniť, tým väčšia zodpovednosť za následky prípadných kybernetických incidentov bude na neho - prostredníctvom zmluvy - prenesená vrátane možných finančných postihov.

Fáza výberu

V tejto fáze musí dodávateľ poskytnúť organizácii minimálne nasledovné dokumenty alebo stanoviská k úrovni informačnej bezpečnosti svojho produktu alebo služby:

- všeobecné prehlásenie o bezpečnosti produktu alebo služby (možnosť A),
- aplikovanie zásad najlepšej bezpečnostnej praxe (možnosť B),
- predloženie výsledkov analýzy rizík (možnosť C).

Fáza nasadzovania

V tejto fáze a podľa typu produktu alebo služby sa od dodávateľa požaduje predložiť výsledky testov na technické zraniteľnosti (možnosť D), prípadne bezpečnostný audit alebo penetračný test (možnosť E) alebo výsledok modelovania kybernetických hrozieb (možnosť F).

b) Spôsoby preukazovania splnenia požiadaviek na informačnú bezpečnosť treťou stranou.

Výsledky testov, auditov alebo modelovania sa musia zameriavať na tie oblasti funkcionality a bezpečnostných opatrení, ktoré boli po dohode s dodávateľom identifikované ako relevantné pre daný produkt alebo službu z pohľadu zaručenia informačnej bezpečnosti.

Tieto výsledky sú následne jedným z hlavných podkladov pre rozhodnutie o akceptovaní produktu alebo služby a o ich uvedení do prevádzky.

Bez ohľadu na spôsob preukazovania splnenia bezpečnostných požiadaviek, musí tretia strana počítať s tým, že zmluva o dodaní produktu alebo služby bude vždy mať aj špecifickú prílohu o kybernetickej bezpečnosti (Bezpečnostné požiadavky na komerčný produkt alebo službu (Vzor prílohy A)), ktorá bude obsahovať relevantné požiadavky v súlade s najlepšou praxou kybernetickej bezpečnosti (ISO, NIST, CISA) a Vyhláškou č. 362/2018 Z.z. NBÚ, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Okrem toho, v prípade, ak zamestnanci tretej strany budú počas nevyhnutnej doby súčasťou informačno-komunikačného prostredia organizácie, budú musieť podpísať a dodržiavať bezpečnostnú smernicu IB-SM-09 Poučenie o zásadách informačnej bezpečnosti pre tretie strany. Podobne v prípade, že dodávateľ bude požadovať vzdialený prístup, bude sa tento riadiť bezpečnostným štandardom organizácie IB-ST-09 Vzdialený prístup k informačným zdrojom pre tretie strany. V oboch prípadoch, tak smernica ako aj štandard, obsahujú len štandardné požiadavky podľa najlepšej praxe, ktoré sa dohodnú špecificky podľa kontextu a vnímaných rizík.

Podľa kritickosti informačného systému alebo komponentu základnej služby musí tretia strana vedieť preukázať záruky kybernetickej bezpečnosti jedným alebo viacerými z nasledovných spôsobov.

Všeobecné prehlásenie o bezpečnosti produktu alebo služby (A)
Tretia strana urobí formálne vyhlásenie o bezpečnosti alebo bezpečnostných vlastnostiach svojho produktu alebo služby (dôvernosť, integrita, dostupnosť, nepopierateľnosť vykonaných aktivít) tým, že predloží zoznam všetkých bezpečnostných opatrení, ktoré boli pri dizajne produktu alebo služby nasadené alebo brané do úvahy.

Toto vyhlásenie má o tým väčšiu výpovednú hodnotu, čím od dodávateľa nezávislejšie je potvrdenie o postupoch, ktoré boli aplikované, napr. formou externého auditu. Pri tomto spôsobe preukazovania sa odporúča spomenúť aj akékoľvek všeobecne známe a overiteľné postupy riadenia kvality.

Najlepšia bezpečnostná prax (B)
Pri demonštrovaní bezpečnosti produktu alebo služby môže tretia strana odkazovať aj na všeobecne známe a teda bežne dostupné postupy tzv. najlepšej praxe, ktorú môžu predstavovať napr. štandardy, checklisty alebo odporúčania ako sú ISO/IEC 27001:2013, ISO/IEC 27019:2017 OWASP, CIS, PCI DSS, NIST SP alebo dokumentácia k bezpečnému nasadzovaniu, konfigurácii alebo prevádzke od výrobcov jednotlivých komponentov produktu alebo služby.

V prípade odkazovania na štandardy najlepšej praxe, je treba vždy podrobnejšie vysvetliť, ktorá časť tejto praxe a v akom rozsahu bola pre daný produkt alebo službu bola aplikovaná.

Napríklad, pri odkazovaní na certifikáciu podľa ISO/IEC 27001 je treba uviesť, aký bol skutočný rozsah certifikácie a ako tento súvisí s daným produktom alebo službou. Pri odkazovaní na dokumentáciu od výrobcu niektorého z komponentov produktu alebo služby (napr. pri Oracle databáze, a pod.), je treba spomenúť konkrétny dokument výrobcu, podľa ktorého dodávateľ postupoval (Oracle® Database Security Guide 19c, E96299-10).

Podobne, ak bol produkt alebo služba posúdená z pohľadu napr. požiadaviek štandardu NIST SP 800-82 alebo ISO/IEC 27019:2017, dodávateľ poskytne zoznam všetkých bezpečnostných opatrení, ktoré boli posudzované.

Výsledky analýzy rizík (C)
Inou možnosťou, ako môže tretia strana zvýšiť dôveru v bezpečnosť ňou dodávaného produktu alebo služby, je poskytnúť organizácii výsledok formálnej analýzy rizík. Takúto analýzu môže vykonať sám dodávateľ alebo akákoľvek odborne spôsobilá a nezávislá strana, len musí byť vždy zrejmé, ktoré hrozby relevantné z hľadiska konkrétneho používania produktu alebo služby, boli posudzované a akými opatreniami boli príslušné zraniteľnosti minimalizované.
Čím známejšia metodika bola pri tom použitá (OCTAVE, CORAS, CRAMM, EBIOS, COBRA, IRAM/ISF, RA2 atď), tým väčšiu hodnotu má takáto správa.

Stav technických zraniteľností (D)
Ďalšou z možností, ako môže tretia strana demonštrovať bezpečnosť svojho produktu alebo služby, je štandardizované posúdenie technických zraniteľností, teda prostredníctvom procesu identifikácie, kvantifikácie a prioritizácie zraniteľností v systéme, produkte alebo službe.
To je možné dosiahnuť aplikovaním vhodných testovacích nástrojov v rôznej fáze životného cyklu produktu alebo služby:

- vo fáze vývoja napr. statickou analýzou zdrojového kódu, SAST (Static Application Security Testing), napr. nástrojmi ako Checkmarx, Kiuwan,
- vo fáze testovania napr. interaktívnou analýzou zdrojového kódu, IAST (Interactive Application Security Testing), napr. nástrojmi ako Seeker (Synopsis),
- vo fáze prevádzky potom dynamickou analýzou zdrojového kódu, DAST (Dynamic Application Security Testing), napr. nástrojmi ako Netsparker, Acunetix, AppScan, alebo sieťovými scannermi ako nmap, OpenVAS, Nessus.

Ako minimum v tejto oblasti sa však požaduje predložiť dokumentáciu o technických zraniteľnostiach a spôsobe nasadzovania bezpečnostných záplat:

- najnovšiu dostupnú správu o stave technických zraniteľností produktu alebo služby (napr. scan na technické zraniteľnosti)
- dokumentáciu o nasadzovaní bezpečnostných záplat

Ak produkt alebo služby využíva štandardné, komerčne dostupné komponenty od iných výrobcov, musia správa o technických zraniteľnostiach a dokumentácia o nasadzovaní záplat zahŕňať aj tieto komponenty alebo súčasti produktu alebo služby.

Bezpečnostný audit / penetračný test (E)
Tretia strana môže pri preukazovaní bezpečnosti svojho produktu alebo služby použiť bezpečnostný audit alebo penetračný test nezávislej tretej strany.

Audit musí byť zameraný na tie relevantné bezpečnostné vlastnosti, ktoré by v podmienkach nasadenia produktu alebo služby v organizácii mali minimalizovať bezpečnostné riziká ohrozujúce základné služby organizácie.

Pri použití penetračného testu musí byť zrejmé, ktoré bezpečnostné scenáre alebo možné zlyhania boli overované a tiež, ktoré špecifické prípady neboli predmetom testu, napr. získanie neoprávneného prístupu, vykonanie aktivity pod identitou iného používateľa, zahladenie stôp po vykonanej operácii alebo zničenie kritických dát.

Modelovanie hrozieb (F)
Modelovanie bezpečnostných hrozieb je postup pri posudzovaní možných hrozieb uvedením zoznamu všetkých možností založených na príležitosti, motivácii alebo technických prostriedkoch, ktoré má potenciálny útočník k dispozícii. Model hrozieb dovoľuje určiť profil ohrozenia systému z pohľadu útočníka.

Typicky sa aplikuje bez posudzovania dopadu vybraných hrozieb, pretože sa pri nich vopred predpokladá veľký až katastrofický dopad. Najčastejšie sa používa pri neštandardných produktoch alebo službách, ktoré boli zostrojené na špecifický, unikátny účel.

c) Prehľad možností preukazovania súladu s bezpečnostnými požiadavkami

Referencia	**Spôsob preukazovania**	**Kto poskytuje/ vykonáva**	**Fáza**
A	Všeobecné prehlásenie o bezpečnosti produktu alebo služby	dodávateľ / dodávateľ	výber (tender)
B	Najlepšia prax kybernetickej bezpečnosti	dodávateľ / dodávateľ	výber (tender)
C	Výsledky analýzy rizík	dodávateľ / dodávateľ	výber (tender)
D	Stav technických zraniteľností	organizácia / organizácia alebo dodávateľ	nasadzovanie/ akceptácia
E	Bezpečnostný audit/ penetračný test	organizácia / organizácia alebo dodávateľ	nasadzovanie/ akceptácia
F	Modelovanie hrozieb	organizácia alebo dodávateľ / organizácia alebo dodávateľ	nasadzovanie/ akceptácia

d) Ostatné bezpečnostné smernice alebo štandardy kybernetickej bezpečnosti PZS

PZS môže poskytnúť Dodávateľovi, s ktorým uzavrie dohodu, aj ďalšie bezpečnostné smernice alebo štandardy, ktoré môžu byť aplikovateľné pre daný druh činnosti alebo prác.

Všetky tieto bezpečnostné požiadavky vychádzajú z najlepšej praxe kybernetickej bezpečnosti a nebudú pre Dodávateľa predstavovať žiadne skryté, nepredvídané náklady ani zásadné prekážky v dodaní diela.