# Zmluva o zabezpečení

# plnenia bezpečnostných opatrení a notifikačných povinností

uzavretá podľa

*§ 269 ods. 2 Zákona č. 513/1991 Z. z. Obchodný zákonník (ďalej len ako „OBZ“),*

*§ 19 a nasl. Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len ako „Zákon o kybernetickej bezpečnosti“),*

*§ 9 a nasl. 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 (ďalej len ako „Vyhláška NBÚ“)*

(ďalej len „Zmluva o kybernetickej bezpečnosti“ alebo „zmluva“)

|  |  |
| --- | --- |
| medzi: | |
| Obchodné meno: | SPP – distribúcia, a.s. |
| Sídlo: | Plátennícka 19013/2, 821 09 Bratislava – mestská časť Ružinov |
| IČO: | 35 910 739 |
| Zapísaná v: | Obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka č. 3481/B |
| DIČ: | 2021931109 |
| IČ DPH: | SK2021931109 |
| Bankové spojenie: | VÚB, a.s. |
| Číslo účtu: | 1119353/0200 |
| SWIFT (BIC): | SUBASKBX |
| IBAN: | SK74 0200 0000 0000 0111 9353 |
| Zastúpená: |  |
|  | |
| (ďalej len „Objednávateľ” alebo „SPP – D“) | |
| A | |
| Obchodné meno: |  |
| Sídlo: |  |
| IČO: |  |
| Zapísaná v: |  |
| DIČ: |  |
| IČ DPH: |  |
| Bankové spojenie: |  |
| Číslo účtu: |  |
| SWIFT (BIC): |  |
| IBAN: |  |
| Zastúpená: |  |
|  | |
| (ďalej len „Dodávateľ”) | |
| (ďalej spolu tiež „zmluvné strany” alebo osobitne „zmluvná strana”) | |

**Článok I**

**Úvodné ustanovenia**

* 1. SPP-D je v zmysle Zákona o kybernetickej bezpečnosti prevádzkovateľom základnej služby zapísaným v registri prevádzkovateľov základnej služby, ktorý prevádzkuje kritickú základnú službu (v sektore energetika v podsektore plyn).
  2. Zmluvné strany uzavreli dňa .............................. zmluvu o .............................. ev.č. ........................, predmetom ktorej je záväzok Dodávateľa poskytovať Objednávateľovi službu, ktorou je ................................ v rozsahu v zmysle zmluvy, najmä avšak nielen špecifikácie uvedenej v príslušnej prílohe zmluvy, inak v rozsahu potrebnom na zabezpečenie splnenia účelu zmluvy (ďalej len „Zmluva“/„Rámcová zmluva“). Zmluvné strany môžu na základe Rámcovej zmluvy uzatvárať osobitnú zmluvu alebo osobitné zmluvy alebo môžu uzatvárať na základe objednávky tzv. Čiastkové zmluvy (ďalej len „Iné zmluvné dojednania“ alebo „Iné zmluvné dojednanie“).
  3. Zmluvné strany potvrdzujú, že Dodávateľ na základe Zmluvy vykonáva činnosti, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Objednávateľa ako prevádzkovateľa kritickej základnej služby, a že Dodávateľ nie je prevádzkovateľom základnej služby/kritickej základnej služby alebo že riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Objednávateľ prostredníctvom Dodávateľa nie je nízke, a preto sú zmluvné strany povinné postupovať podľa Zákona o kybernetickej bezpečnosti a uzavrieť Zmluvu o kybernetickej bezpečnosti za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností, pri uzatvorení Zmluvy o kybernetickej bezpečnosti sa vykonáva analýza rizík.
  4. Dodávateľ je v zmysle § 19 ods. 2 Zákona o kybernetickej bezpečnosti počas trvania zmluvného vzťahu s Objednávateľom povinný vykonávať a realizovať bezpečnostné opatrenia v súlade s  touto zmluvou a Zákonom o kybernetickej bezpečnosti a je povinný podrobiť sa kontrole plnenia týchto opatrení zo strany Objednávateľa a v prípade zmluvného vzťahu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu, t.j. s Objednávateľom kontrolu Dodávateľa môže vykonávať aj Národný bezpečnostný úrad (ďalej len „NBÚ“); na tento účel má Dodávateľ postavenie prevádzkovateľa základnej služby.
  5. Objednávateľ je v zmysle § 19 ods. 7 Zákona o kybernetickej bezpečnosti povinný hlásiť NBÚ informáciu o uzatvorení zmluvy s treťou stranou o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti a aj informáciu o jej ukončení. Dodávateľ berie na vedomie, že v zmysle § 17 ods. 1 písm. i) Zákona o kybernetickej bezpečnosti sa tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu, zapisuje do registra prevádzkovateľov základnej služby a to za podmienok a spôsobom uvedeným v § 17 Zákona o kybernetickej bezpečnosti.

* 1. Účelom tejto zmluvy je stanoviť základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť a udržať kybernetickú bezpečnosť a odolnosť sietí a informačných systémov Objednávateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Objednávateľa a minimalizovať vplyv kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania základnej služby zo strany Objednávateľa, a to aj v spolupráci s Dodávateľom.
  2. Plnenie povinností podľa Zmluvy o kybernetickej bezpečnosti tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Objednávateľa a to po celú dobu trvania Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní.
  3. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu nadobudnutia účinnosti Zmluvy o kybernetickej bezpečnosti až do skončenia platnosti Zmluvy/Rámcovej zmluvy a Iných zmluvných dojednaní, pokiaľ z právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti Zmluvy/Rámcovej zmluvy a Iných zmluvných dojednaní.
  4. Odplata za plnenie povinností Dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Objednávateľom Dodávateľovi podľa Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy od Objednávateľa nemá nárok.

1.10 Pojmy používané v tejto zmluve majú význam im priradený v Zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

**Článok II**

**Predmet Zmluvy**

* 1. Predmetom tejto zmluvy je úprava práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností tak, aby bola zaistená kybernetická bezpečnosť na požadovanej úrovni a  spôsobilosť predchádzať a odolávať kybernetickým bezpečnostným incidentom a vzniknuté kybernetické bezpečnostné incidenty riadne hlásiť a riešiť a minimalizovať ich vplyv na siete a informačné systémy.
  2. Rozsah činností, ktoré Dodávateľ vykonáva pre Objednávateľa, je definovaný predovšetkým v Zmluve/Rámcovej zmluve/Iných zmluvných dojednaniach a v príslušných právnych predpisoch, ktoré sa na poskytovanie služby vzťahujú.
  3. Dodávateľ vyhlasuje, že k dátumu podpisu tejto zmluvy má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie účelu tejto zmluvy.

**Článok III**

**Práva a povinnosti Dodávateľa**

**Všeobecné opatrenia**

* 1. Dodávateľ sa zaväzuje pri poskytovaní služby v zmysle bodu 1.2 tejto zmluvy oboznámiť sa, prijímať a dodržiavať bezpečnostné politiky predložené Objednávateľom, a to predovšetkým bezpečnostné politiky obsiahnuté v smernici Objednávateľa *Bezpečnosť informačných a komunikačných systémov SPP – distribúcia, a.s.,* ktoré boli Dodávateľovi poskytnuté pred uzavretím tejto zmluvy a s ktorými mal možnosť sa oboznámiť a podpisom tejto zmluvy vyjadruje Dodávateľ s nimi súhlas.
  2. Dodávateľ berie na vedomie a súhlasí s tým, že bezpečnostné politiky Objednávateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Objednávateľa a aktuálnym hrozbám, ktoré by mohli mať potenciálny nepriaznivý vplyv na kritickú základnú službu Objednávateľa. Pri každej zmene bezpečnostných politík je Objednávateľ bez zbytočného odkladu poskytnúť aktualizované/zmenené bezpečnostné politiky Dodávateľovi.
  3. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti, ktorých špecifikácia a rozsah je uvedený v tejto zmluve tak, aby boli naplnený účel tejto zmluvy. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami.
  4. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu a spôsobom uvedeným v tejto zmluve tak, aby boli naplnený účel tejto zmluvy najmä bezodkladne informovať Objednávateľa o každom podozrení na kybernetický bezpečnostný incident a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti poskytovaných služieb, hlásiť všetky potrebné informácie požadované Objednávateľom pri zabezpečovaní požiadaviek kladených na Objednávateľa podľa Zákona o kybernetickej bezpečnosti alebo Vyhlášky NBÚ, hlásiť všetky informácie, ktoré majú vplyv na túto zmluvu.
  5. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Objednávateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.
  6. Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na kritickú základnú službu Objednávateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
  7. Dodávateľ je povinný počas trvania tejto zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej, technologickej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie účelu tejto zmluvy.
  8. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Objednávateľovi na nahliadnutie a zhotovenie kópií.
  9. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy a v súlade so Zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, s najnovšími bezpečnostnými trendami a medzinárodnými normami 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, bezpečnostnými metodikami, politikami a zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva NBÚ v oblasti kybernetickej bezpečnosti.
  10. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto zmluvy v súlade so sektorovými  
      bezpečnostnými opatreniami, ktoré vydáva Ministerstvo hospodárstva Slovenskej republiky v spolupráci s NBÚ.
  11. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto zmluvy na zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
  12. Dodávateľ sa zaväzuje dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť Objednávateľa mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
  13. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy bezodkladne, pokiaľ to nie je v tejto zmluve alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.

**Bezpečnostné opatrenia**

* 1. Dodávateľ sa zaväzuje pri poskytovaní služieb Objednávateľovi prijať a dodržiavať bezpečnostné opatrenia a požiadavky za podmienok (najmä na základe rizikovej analýzy), spôsobom a v rozsahu Zákona o kybernetickej bezpečnosti (najmä pre oblasť podľa ustanovení § 20 ods. 3 písm. d), g) až i), k) a m)), Vyhlášky NBÚ (najmä podľa ustanovení § 8, § 11, § 12, § 13, § 15, § 17), a iných právnych predpisov vydaných v súlade so Zákonom o kybernetickej bezpečnosti a v rozsahu špecifikovanom v bezpečnostných politikách Objednávateľa a tak, aby bolo zabezpečené dosiahnutie nasledovných cieľov: identifikovať zraniteľnosti, kybernetické hrozby a riziká, chrániť preventívne informačné aktíva pred kybernetickou hrozbou a zabrániť vzniku kybernetického bezpečnostného incidentu, detegovať kybernetické bezpečnostné incidenty, reagovať na identifikované zraniteľnosti a kybernetické bezpečnostné incidenty a minimalizovať ich vplyv na siete a informačné systémy, obnoviť siete a informačné systémy, napraviť negatívne dopady po vzniku kybernetického bezpečnostného incidentu a uviesť poskytované služby do stavu plynulého a nerušeného poskytovania.
  2. Dodávateľ sa zaväzuje informovať Objednávateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
  3. Pre oblasť riadenia prístupov osôb k sieti a informačnému systému realizuje Dodávateľ opatrenia podľa ustanovenia § 8 Vyhlášky NBÚ, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

1. Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.
2. Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb Objednávateľa, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
3. Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.
4. Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
5. Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
6. Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).
7. 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.
8. Zmluvné strany potvrdzujú, že Dodávateľa na základe Zmluvy vykonáva činnosti, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Objednávateľa ako prevádzkovateľa základnej služby a sú povinné postupovať podľa Zákona o kybernetickej bezpečnosti a uzavrieť Zmluvu o kybernetickej bezpečnosti za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností.
   1. Pre oblasť hodnotenia zraniteľností a bezpečnostných aktualizácií a ochrany proti škodlivému kódu realizuje Dodávateľ opatrenia podľa ustanovenia § 11 a § 12 Vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Objednávateľovi a ktoré toto poskytovanie služieb Objednávateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:
9. Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb,
10. Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb,
11. Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.
    1. Pre oblasť riešenia sieťovej a komunikačnej bezpečnosti realizuje Dodávateľ opatrenia podľa ustanovenia § 13 Vyhlášky NBÚ, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:
12. Riadenie prístupov používateľov k sieťam a informačným systémom,
13. Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Objednávateľa, ktoré využíva pri poskytovaní služieb Objednávateľovi, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
14. Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií,
15. Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,
16. Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete,
17. Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov,
18. Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu,
19. Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
20. Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
21. Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje,
22. Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty,
23. Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
24. Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
25. Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
26. Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
27. Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.
    1. Pre oblasť zaznamenávania udalostí a monitorovania realizuje Dodávateľ opatrenia podľa ustanovenia § 15 Vyhlášky NBÚ v rozsahu potrebnom pre poskytovanie služieb v súlade s príslušnými právnymi predpismi, ktoré sa na poskytovanie služby vzťahujú.
    2. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Dodávateľ opatrenia podľa ustanovenia § 17 Vyhlášky NBÚ, najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na poskytovanie služieb Objednávateľovi. To zahŕňa napríklad prijatie opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:
28. Oboznámenie sa s postupmi Objednávateľa pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči Objednávateľovi.
29. Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Objednávateľovi,
30. Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
31. Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.
32. Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Objednávateľa.
33. Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Objednávateľom.

**Personálne opatrenia**

* 1. Dodávateľ je povinný doručiť Objednávateľovi do 7 pracovných dní od uzavretia tejto zmluvy zoznam pracovných rolí a zoznam osôb (zamestnanci Dodávateľa, subdodávatelia a ich zamestnanci), ktoré sa budú podieľať na plnení Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní a tejto zmluvy alebo budú mať prístup k informáciám Objednávateľa, ktorý sa jeho doručením Objednávateľovi stane súčasťou tejto zmluvy. Každú zmenu v personálnom obsadení je Dodávateľ povinný Objednávateľovi písomne oznámiť vopred, pričom pre doručenie zoznamu a oznamovanie zmien v zozname sa použijú ustanovenia zmluvy o doručovaní (bod 6.1), s tým, že Dodávateľ zároveň tieto doručí aj elektronicky na adresu uvedenú v bode 6.3; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve.
  2. V zozname budú označené osoby v rozsahu: meno a priezvisko, rola, proces súvisiaci s prevádzkou základnej služby, pracovné zaradenie, e-mailová adresa a telefónne číslo, názov zamestnávateľa v prípade osôb vykonávajúcich činnosť pre Dodávateľa, ktorí nie sú v pracovnoprávnom vzťahu aj meno osoby zodpovednej za mimopracovný zmluvný vzťah. Dodávateľ je povinný odovzdať zoznam osôb, ktorí nie sú v pracovnoprávnom vzťahu s Dodávateľom, Objednávateľovi s výslovným písomným súhlasom dotknutých osôb so spracovaním osobných údajov v súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). Pri porušení tejto povinnosti Dodávateľ nesie plnú zodpovednosť za ochranu osobných údajov dotknutých osôb. Objednávateľ sa zaväzuje, že bude spracovávať tieto osobné údaje len pre potreby plnenia tejto zmluvy a zachovania bezpečnosti infraštruktúry podľa Zákona o kybernetickej bezpečnosti po dobu trvania účelu spracúvania.
  3. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa § 12 ods. 1 Zákona o kybernetickej bezpečnosti a článku V tejto zmluvy osoby, ktoré sa budú podieľať na plnení podľa bodu 3.21 tejto zmluvy.

**Článok IV**

**Kybernetické bezpečnostné incidenty**

**Prevencia kybernetických bezpečnostných incidentov**

* 1. Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na kritickú základnú službu Objednávateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa (ďalej len „incidenty):

1. zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Objednávateľa,
2. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní a tejto zmluvy alebo budú mať prístup k informáciám Objednávateľa,
3. sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
4. sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa,
5. predchádzať vzniku incidentov,
6. systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
7. prijímať od Objednávateľa varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa,
8. zasielať Objednávateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a
9. spolupracovať s Objednávateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa.

**Reaktivita pri riešení kybernetických bezpečnostných incidentov**

* 1. Dodávateľ sa zaväzuje bezodkladne, avšak najneskôr do 20 hodín od zistenia hlásiť Objednávateľovi každý incident a všetky skutočnosti majúce vplyv na zabezpečovanie kybernetickej bezpečnosti Objednávateľa (najmä kybernetický bezpečnostný incident, závažný kybernetický bezpečnostný incident, kybernetickú hrozbu, významnú kybernetickú hrozbu, udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident) spôsobom určeným v nasledujúcich bodoch tejto zmluvy. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
  2. **Hlásenie incidentu a všetkých skutočností majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti** - Dodávateľ nahlasuje Objednávateľovi incidenty elektronicky na adresu:
* elektronicky na adresu: [***csirt.sppd@spp-distribucia.sk***](mailto:csirt.sppd@spp-distribucia.sk)

a zároveň

* telefonicky na telefónne čísla: ***+421 905 497 279*** *alebo* ***+421 915 495 900*** 
  1. **Obsah hlásenia** – hlásenie musí obsahovať minimálne nasledovné informácie:
* Popis bezpečnostného incidentu/ všetkých skutočností majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti
* Typ bezpečnostného incidentu
* Časové údaje zistenia a vzniku incidentu/skutočností majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti
* Zasiahnuté aktíva/služba
* Informáciu, či bol incident nahlásený NBÚ (áno – nie)
* Spôsob odstránenia incidentu
* Popis navrhnutých opatrení na zabránenie opakovaniu incidentu
  1. Dodávateľ sa zaväzuje 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 Objednávateľa spolupracovať s Objednávateľom, NBÚ a ďalším ústredným orgánom alebo iným orgánom štátnej správy určeným v § 4 Zákona o kybernetickej bezpečnosti jednať, a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.
  2. Dodávateľ sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Objednávateľovi.
  3. Dodávateľ sa zaväzuje oznámiť Objednávateľovi skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
  4. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Objednávateľovi vykonanie reaktívneho opatrenia a jeho výsledok.
  5. Po vyriešení incidentu je Dodávateľ na výzvu Objednávateľa v ním určenej lehote povinný predložiť Objednávateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „ochranné opatrenia") na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v lehote, ktorú určí Objednávateľ, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Objednávateľom na jeho návrhu.
  6. Po schválení ochranného opatrenia Objednávateľom, je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní ochranného opatrenia Dodávateľom je Dodávateľ povinný preveriť jeho účinnosť.

**Článok V**

**Mlčanlivosť**

* 1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením tejto zmluvy a Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní, a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti. Dodávateľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základnú službu Objednávateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa. Dodávateľ je zároveň povinný chrániť všetky informácie poskytnuté Objednávateľom Dodávateľovi.
  2. Dodávateľ sa v rovnakom rozsahu zaväzuje zaviazať povinnosťou mlčanlivosti aj všetky ním poverené osoby, ktoré budú zúčastnené na predmete plnenia Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní a tejto zmluvy (t.j. jeho zamestnanci, subdodávatelia a ich zamestnanci). Dodávateľ je povinný na požiadanie preukázať Objednávateľovi splnenie tejto povinnosti. Povinnosť mlčanlivosti trvá aj po zániku ich pracovno-právneho vzťahu alebo obchodného vzťahu.
  3. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.
  4. Výnimky z povinnosti mlčanlivosti podľa tohto článku sú uvedené v § 12 Zákon o kybernetickej bezpečnosti.

**Článok VI**

**Doručovanie a komunikácia**

**Doručovanie**

1. Akékoľvek prejavy vôle zmluvných strán súvisiace so Zmluvou o kybernetickej bezpečnosti najmä odstúpenie od zmluvy, výpoveď zmluvy, návrhy dodatkov k zmluve, zaslanie zoznamu rolí a personálneho obsadenia, oznámenie zmeny údajov podľa zmluvy, budú vyhotovené písomne a doručené druhej zmluvnej strane osobne, poštou alebo kuriérom, ak v Zmluve o kybernetickej bezpečnosti nie je uvedené inak.
2. Všetky písomnosti sa považujú za doručené aj v prípade neprevzatia zásielky (v prípade doručovania poštou alebo kuriérom, napr. ak sa zásielka vráti Objednávateľovi späť s poznámkou „adresát neznámy“, „nevyzdvihnuté v odbernej lehote“, „adresát odmietol zásielku prevziať“, „adresát sa odsťahoval“ alebo inou obdobnou poznámkou znamenajúcou neúspešné doručenie zásielky) odoslanej poštou alebo kuriérom na adresu sídla alebo miesta podnikania druhej zmluvnej strany alebo na adresu uvedenú v záhlaví zmluvy, resp. na adresu oznámenú druhej zmluvnej strane, a to desiatym dňom odo dňa odoslania takejto zásielky alebo pokiaľ sa nedoručená zásielka vráti Objednávateľovi skôr, tak dňom jej vrátenia. Každá zo zmluvných strán je povinná písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu ohľadne doručovania, a to najneskôr do 5 pracovných dní po tom, čo k takejto zmene dôjde. Pokiaľ sa z dôvodu oneskoreného alebo nevykonaného oznámenia o zmene miesta doručovania nepodarí včas a riadne doručiť písomnosť druhej zmluvnej strane, považuje sa deň neúspešného pokusu o opakované doručenie písomnosti za deň doručenia písomnosti druhej zmluvnej strane so všetkými právnymi dôsledkami pre dotknutú zmluvnú stranu.
3. Akékoľvek oznámenie, informácia požadovaná Objednávateľom vymedzená v zmluve, informácia potrebná na plnenie povinností Dodávateľa vyplývajúcich zo zmluvy a Zákona o kybernetickej bezpečnosti, informácie, ktoré by mohli mať vplyv na zmluvu alebo iná formálna korešpondencia podľa Zmluvy o kybernetickej bezpečnosti, sa doručuje na adresy uvedené v tomto článku alebo na iné adresy, ktoré si zmluvné strany navzájom oznámia doručením na adresu uvedenú v tomto článku.

Objednávateľovi elektronicky na adresu: [csirt.sppd@spp-distribucia.sk](mailto:csirt.sppd@spp-distribucia.sk)

Dodávateľovi elektronicky na adresu: [●]

1. V prípade doručovania podľa predchádzajúceho bodu, druhá zmluvná strana bezodkladne potvrdí doručenie preukázateľnou formou. Pre vylúčenie pochybností sa uvádza, že nesplnenie tejto povinnosti nezakladá fikciu nedoručenia takejto písomnosti alebo prejavu vôle zmluvnej strany.

**Kontaktné osoby**

1. Na účely vykonávania ustanovení tejto zmluvy sú oprávnenými osobami, resp. kontaktnými osobami (ďalej len „Oprávnené osoby“) nasledovné osoby:

**za Dodávateľa:**

1. Vo veciach kybernetickej bezpečnosti:

[meno, priezvisko, funkcia]

Telefón: [●]

E-mail: [●]

1. Vo veciach zmluvných:

[meno, priezvisko, funkcia]

Telefón: [●]

E-mail: [●]

**za Objednávateľa:**

1. Vo veciach kybernetickej bezpečnosti:

Ing. Slavomír Fedor, špecialista pre komunikácie IT - senior

Telefón: +421 915 495 900

E-mail: [slavomir.fedor@spp-distribucia.sk](mailto:slavomir.fedor@spp-distribucia.sk)

Ing. Miroslav Majerčík, vedúci oddelenia prevádzky IT a SCADA

Telefón: +421 905 497 279

E-mail: [miroslav.majercik@spp-distribucia.sk](mailto:jan.lacho@spp-distribucia.sk)

1. Vo veciach zmluvných:

JUDr. Marián Uhrík, vedúci odd. prevádzkového obstarávania

Telefón: 02/20402112

E-mail: [marian.uhrik@spp-distribucia.sk](mailto:marian.uhrik@spp-distribucia.sk)

1. Zmluvné strany týmto vyhlasujú, že Oprávnené osoby disponujú oprávneniami a právomocami potrebnými pre prijímanie a realizáciu rozhodnutí v súvislosti s plnením tejto zmluvy, avšak Oprávnené osoby zmluvných strán nie sú oprávnené zmluvu meniť ani zrušiť, ak nie je v tejto zmluve uvedené inak.
2. Zmluvné strany môžu zmeniť Oprávnené osoby, táto zmena musí byť oznámená v písomnej forme vopred, pričom pre doručenie sa použijú ustanovenia zmluvy o doručovaní (bod 6.1) ; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve.

**Článok VII.**

**Audit a kontrolné činnosti**

1. Objednávateľ má právo požadovať pravidelné a ad hoc informácie o výkone činnosti Dodávateľa na základe tejto zmluvy vrátane informácií o využívaní tretích osôb Dodávateľom a o ich činnosti.
2. Objednávateľ je oprávnený pravidelne a ad hoc kontrolovať činnosť Dodávateľa vykonávanú na základe tejto zmluvy, vrátane činností vykonávaných pre Dodávateľa tretími osobami. Na tento účel je oprávnený požadovať poskytnutie dokumentov, informácií a vysvetlenia a overovať príslušné skutočnosti v priestoroch Dodávateľa a tretích osôb využívaných Dodávateľom na výkon činností na základe tejto zmluvy, ako v tuzemsku, tak aj v zahraničí.
3. Objednávateľ je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie účelu tejto zmluvy. Každý takýto audit bude dodržiavať primerané bezpečnostné požiadavky Dodávateľa a nebude neprimerane zasahovať do jeho obchodných aktivít.
4. Prípadné nedostatky zistené auditom/kontrolnou činnosťou je Dodávateľ povinný odstrániť, resp. zabezpečiť ich odstránenie bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní od vykonania auditu/kontrolnej činnosti Objednávateľom. O náprave takýchto nedostatkov a o spôsobe ich nápravy Dodávateľ upovedomí Objednávateľa vo vyššie uvedenej lehote, a to v písomnej forme na adresu sídla Objednávateľa uvedenú v záhlaví tejto zmluvy.
5. Dodávateľ sa zaväzuje pri audite/kontrolnej činnosti spolupracovať s Objednávateľom  
   a sprístupniť mu svoje priestory a priestory tretích osôb využívaných Dodávateľom na výkon činností na základe tejto zmluvy, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
6. Objednávateľ môže audit/kontrolnú činnosť u Dodávateľa realizovať sám alebo  
   prostredníctvom tretej osoby; v takom prípade práva a povinnosti Objednávateľa pri výkone auditu/kontrolnej činnosti realizuje Objednávateľom poverená tretia osoba, ktorej je Dodávateľ povinný poskytnúť rovnakú súčinnosť ako Objednávateľovi.
7. Objednávateľ je v rámci auditu/kontrolnej činnosti oprávnený klásť otázky osobám (zamestnanci Dodávateľa, subdodávateľ a jeho zamestnanci), ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
8. V rámci auditu je Dodávateľ povinný preukázať Objednávateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, resp. osôb, ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, záväzok a poučenie svojich zamestnancov, resp. osôb, ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
9. Objednávateľ sa zaväzuje oznámiť Dodávateľovi najmenej desať pracovných dní vopred svoj zámer realizovať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu Objednávateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
10. Objednávateľ sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku V tejto zmluvy sa uplatňujú primerane.
11. Objednávateľ a ním poverené osoby pri návšteve priestorov Dodávateľa v rámci výkonu auditu/kontrolnej činnosti musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len ako „BOZP") a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len ako „PO"), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Objednávateľ. 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 sa zaväzuje preukázateľne informovať Objednávateľa a ním poverené osoby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia, vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

**Článok VIII**

**Subdodávateľ**

1. Objednávateľ je oprávnený zapojiť ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Objednávateľa namiesto Dodávateľa (ďalej len „subdodávateľa“) za splnenia týchto podmienok, ak zo Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní nevyplýva iné:
2. vopred oznámi Objednávateľovi zámer využiť subdodávateľa vrátane špecifikácie spôsobu jeho využitia;
3. Objednávateľ s využitím subdodávateľa udelí písomný súhlas. Objednávateľ si vyhradzuje právo tento písomný súhlas kedykoľvek odvolať a to aj bez uvedenia dôvodov;
4. pred zapojením subdodávateľa zabezpečí Dodávateľ, že táto osoba sa vo vzťahu k výkonu činností na základe Zmluvy o kybernetickej bezpečnosti zmluvne zaviaže v plnom rozsahu dodržiavať všetky práva a povinnosti ako Dodávateľ podľa tejto zmluvy a požiadavky Vyhlášky NBÚ, Zákona o kybernetickej bezpečnosti a jeho ostatných vykonávacích predpisov tak, aby bol naplnený účel tejto zmluvy.
5. Dodávateľ je povinný na požiadane predložiť Objednávateľovi kópiu zmluvy uzavretú so subdodávateľom, ktorou preukáže, že subdodávateľ sa v plnom rozsahu zaviazal dodržiavať všetky práva a povinnosti ako Dodávateľ podľa tejto zmluvy a požiadavky Vyhlášky NBÚ, Zákona o kybernetickej bezpečnosti a jeho ostatných vykonávacích predpisov.
6. Dodávateľ sa zaväzuje zabezpečiť, aby Objednávateľ mohol vykonať audit/kontrolnú činnosť v súlade s ustanoveniami tejto zmluvy aj subdodávateľa. Dodávateľ zodpovedá za konanie subdodávateľa tak, ako keby konal sám.

**Článok IX**

**Porušenie povinností a sankcie**

1. V prípade porušenia akejkoľvek povinnosti, záväzku alebo vyhlásenia Dodávateľa uvedených v tejto zmluve o zabezpečení kybernetickej bezpečnosti, vrátane porušenia povinnosti mlčanlivosti, je Objednávateľ oprávnený požadovať od Dodávateľa zmluvnú pokutu vo výške 5.000 EUR za každý jednotlivý prípad porušenia, a to aj opakovane. Zaplatením zmluvnej pokuty nie je dotknutý nárok Objednávateľa na náhradu škody podľa príslušných právnych predpisov.
2. Zaplatenie zmluvnej pokuty nezbavuje Dodávateľa povinnosti splniť záväzok zabezpečený zmluvnou pokutou.
3. Dodávateľ je povinný informovať Objednávateľa o porušení povinnosti mlčanlivosti a o vykonaných opatreniach na odstránenie následkov porušenia tejto povinnosti bez zbytočného odkladu potom, čo sa o porušení dozvedel. Dodávateľ je povinný odstrániť, resp. v maximálnej možnej miere minimalizovať následky porušenia povinnosti mlčanlivosti, bez zbytočného odkladu potom, čo sa o porušení dozvedel.
4. V prípade, ak Dodávateľ spôsobí Objednávateľovi porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. OBZ. Pre odstránenie právnych pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Objednávateľovi tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.
5. V prípade, ak orgán príslušný konať vo veciach kybernetickej bezpečnosti uloží Objednávateľovi v dôsledku porušenia akejkoľvek povinnosti, záväzku alebo vyhlásenia Dodávateľa vyplývajúcich z tejto zmluvy pokutu, alebo inú sankciu, Dodávateľ je povinný nahradiť túto Objednávateľovi v plnej výške a to do 30 dní odo dňa doručenia výzvy Objednávateľa na jej náhradu.

**Článok X**

**Trvanie zmluvy**

1. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania hlavného zmluvného vzťahu založeného Zmluvou/Rámcovou zmluvou/Iným zmluvným dojednaním.
2. Porušenie nižšie uvedených povinností Dodávateľom sa považuje za podstatné porušenie zmluvy a zároveň aj za podstatné porušenie Zmluvy/Rámcovej zmluvy/Iného zmluvného dojednania a je dôvodom na okamžité odstúpenie od Zmluvy/Rámcovej zmluvy/Iného zmluvného dojednania:
3. Dodávateľ neprijme a/alebo nedodržiava bezpečnostné politiky predložené Objednávateľom v zmysle ustanovenia bodu 3.1 zmluvy,
4. Dodávateľ neprijme a/alebo nedodržiava bezpečnostné opatrenia na úseku kybernetickej bezpečnosti, ktorých špecifikácia a rozsah je uvedený v tejto zmluve v zmysle ustanovenia bodu 3.3 a 3.14 a nasl. zmluvy,
5. Dodávateľ nestanoví postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii a/alebo ju neaktualizuje v zmysle ustanovenia bodu 3.8 zmluvy,
6. Dodávateľ neumožní vykonať audit v zmysle ustanovenia bodu 7.9 zmluvy,
7. Dodávateľ poruší povinnosti uvedené v čl. IV týkajúce sa kybernetických bezpečnostných incidentov,
8. Dodávateľ poruší povinnosti uvedené v čl. V týkajúce sa mlčanlivosti.
9. Ukončením zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce zo zmluvy okrem povinností týkajúcich sa mlčanlivosti, nárokov na náhradu škody, nárokov na zmluvné alebo zákonné sankcie, resp. iných práv a povinností, ak to vyplýva z ich charakteru v zmysle príslušných právnych predpisov.
10. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej kritickej základnej služby na Objednávateľa. Tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu a to po dobu piatich rokov po ukončení tejto zmluvy.
11. Po ukončení tejto zmluvy je Dodávateľ povinný vrátiť alebo previesť na Objednávateľa všetky informácie, ku ktorým mal počas trvania tohto zmluvného vzťahu prístup, resp. tieto podľa pokynu Objednávateľa zničiť.

**XI**

**Záverečné ustanovenia**

1. Táto zmluva nadobúda platnosť a účinnosť dňom jej podpísania oboma zmluvnými stranami.
2. Táto zmluva sa po jej podpísaní stáva integrálnou súčasťou Zmluvy/Rámcovej zmluvy/Iných zmluvných dojednaní.
3. Práva a povinnosti zmluvných strán neupravené v tejto zmluve sa riadia Zmluvou/Rámcovou zmluvou/Inými zmluvnými dojednaniami, Vyhláškou NBÚ alebo inými právnymi predpismi vydanými v súlade so Zákonom o kybernetickej bezpečnosti a so Zákonom o kybernetickej bezpečnosti.
4. Táto zmluva sa môže meniť alebo dopĺňať iba dohodou zmluvných strán v písomnej forme, ak zo zmluvy nevyplýva niečo iné.
5. Prípadné spory vyplývajúce z tejto zmluvy budú riešené predovšetkým mimosúdne. Podpisom tejto zmluvy zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.
6. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto zmluvy na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
7. V prípade, že niektoré z ustanovení tejto zmluvy sa stane neplatným, neúčinným alebo nevykonateľným, zostáva platnosť ostatných ustanovení nedotknutá. Ak nastane takáto situácia, zmluvné strany sa písomne dohodnú na riešení, ktoré zachová kontext a účel daného ustanovenia.
8. Zmluvné strany týmto vyhlasujú, že s obsahom tejto zmluvy súhlasia, a že vyjadruje ich slobodnú a vážnu vôľu, ich zmluvná voľnosť nie je obmedzená a na znak súhlasu s jej obsahom túto podpisujú.
9. Osoby, ktoré podpisujú zmluvu vyhlasujú, že sú oprávnené konať v mene zmluvnej strany a zaväzovať zmluvnú stranu svojim podpisom.
10. Táto zmluva je vyhotovená v 4 rovnopisoch s platnosťou originálu, pre každú zmluvnú stranu 2 vyhotovenia.
11. Dodávateľ svojím podpisom potvrdzuje, že mu boli poskytnuté informácie o spracúvaní osobných údajov Objednávateľom v rozsahu stanovenom právnymi predpismi upravujúcimi ochranu osobných údajov obsiahnuté v dokumente dostupnom na http://www.spp-distribucia.sk/sk\_gdpr a že zabezpečil poskytnutie týchto informácií osobám, ktorých osobné údaje Objednávateľovi poskytol.

|  |  |
| --- | --- |
| V ............................, dňa | V ....................., dňa ..................... |
| Dodávateľ: | Objednávateľ: |