Číslo zmluvy:

# Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

# uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a podľa § 7 ods. 2 vyhlášky Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach (ďalej len „Vyhláška o bezpečnostných opatreniach“)

# (ďalej len „Zmluva KB“)

medzi zmluvnými stranami:

Obchodné meno: **Národná diaľničná spoločnosť, a. s.**

Sídlo: Dúbravská cesta 14, 841 04 Bratislava

Právna forma: akciová spoločnosť zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka číslo: 3518/B

Štatutárny orgán: predstavenstvo zastúpené:

Ing. Filip Macháček, predseda predstavenstva a generálny riaditeľ

Ing. Július Mihálik, člen predstavenstva

Bankové spojenie: Štátna pokladnica

Číslo účtu: SK95 8180 0000 0070 0069 4593, SWIFT: SPSRSKBA,

IČO: 35 919 001

IČ DPH: SK 202 193 7775

Tel./Fax: 02/583 11 111, 02/583 11 701

(ďalej len „**Prevádzkovateľ základnej služby**“ alebo aj „**PZS**“)

a

**Zhotoviteľ:**

Obchodné meno:

Sídlo:

Právna forma:

Štatutárny orgán:

Bankové spojenie:

Číslo účtu:

IČO:

IČ DPH:

Tel./Fax:

(ďalej len „**Zhotoviteľ**“)

(Prevádzkovateľ základnej služby a Zhotoviteľ spolu ďalej len „**zmluvné strany**“)

**Článok I.**

ÚVODNÉ USTANOVENIA

1. **Národná diaľničná spoločnosť, a. s.** je podľa § 17, ods. 1 písm. b a c zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB“) **prevádzkovateľom kritickej základnej služby Centrálny riadiaci systém tunela a Informačný systém diaľnic a rýchlostných ciest.**
2. Zhotoviteľ je treťou stranou podľa § 19 ods. 2 v spojení s § 5 ods. 1 písm. ad) Zákona o kybernetickej bezpečnosti.
3. Prevádzkovateľ základnej služby a Zhotoviteľ uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „Zmluva KB“) s cieľom špecifikovať plnenie bezpečnostných opatrení a notifikačných povinností podľa ZoKB v nadväznosti na zmluvu **Zmluva o dielo - ......zo dňa ......** (ďalej len „**hlavná zmluva**“) na výkon činností, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa základnej služby.
4. Plnenie povinností podľa tejto Zmluvy KB sa vyžaduje počas celej doby trvania hlavného zmluvného vzťahu medzi Zhotoviteľom a Prevádzkovateľom základnej služby, pričom táto Zmluva KB trvá najneskôr dovtedy, pokiaľ bude trvať hlavný zmluvný vzťah medzi Zhotoviteľom a Prevádzkovateľom základnej služby.

**Článok II.**

**PREDMET ZMLUVY**

1. Predmetom tejto Zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona o kybernetickej bezpečnosti Zhotoviteľom počas celej doby výkonu činností, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Prevádzkovateľa základnej služby.
2. Miestom plnenia tejto Zmluvy sú najmä pracoviská Prevádzkovateľa základnej služby a pracoviská Zhotoviteľa.

**Článok III.**

**ZÁVÄZOK ZHOTOVITEĽA A PREVÁDZKOVATEĽA ZÁKLADNEJ SLUŽBY**

1. Zhotoviteľ sa zaväzuje počas trvania zmluvného vzťahu vykonávať a realizovať bezpečnostné opatrenia v súlade s touto Zmluvou, ZoKB a Vyhláškou o bezpečnostných opatreniach. Zhotoviteľ na účely plnenia povinností podľa prvej vety tohto bodu Zmluvy vyhlasuje, že sa oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení, ktoré tvoria Prílohu č. 2 tejto zmluvy.
2. Zhotoviteľ sa zaväzuje riadiť sa stanovenými bezpečnostnými opatreniami v tejto Zmluve KB.
3. Zhotoviteľ sa zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby podľa § 2 písm. d) Vyhlášky o bezpečnostných opatreniach v rozsahu potrebnom na plnenie povinností vyplývajúcich mu z tejto Zmluvy. Zhotoviteľ na účely plnenia povinnosti podľa tejto Zmluvy vyhlasuje, že sa oboznámil s bezpečnostnými politikami Prevádzkovateľa základnej služby v rozsahu na to potrebnom. V uvedenom prípade sa jedná o bezpečnostné politiky, ktorých nevyhnutný obsah nie je súčasťou Prílohy č.2 tejto Zmluvy.
4. Zhotoviteľ  berie na vedomie, že požadované opatrenia z bezpečnostných politík Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa kritickej základnej služby a aktuálnym hrozbám dotýkajúcim sa Zhotoviteľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby. Prevádzkovateľ základnej služby sa zaväzuje o takýchto plánovaných zmenách Zhotoviteľa informovať najneskôr 30 (tridsať) dní pred ich implementovaním.
5. Zhotoviteľ sa zaväzuje plniť všetky notifikačné povinnosti voči Prevádzkovateľovi základnej služby, aby Prevádzkovateľ základnej služby mohol plniť svoje povinnosti vyplývajúce zo Zákona o kybernetickej bezpečnosti riadne a včas.
6. Zhotoviteľ sa zaväzuje bezodkladne informovať Prevádzkovateľa základnej služby o každom kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti Prevádzkovateľa základnej služby, o ktorých sa dozvie, a to spôsobom určeným touto Zmluvou. Zhotoviteľ určuje závažnosť kybernetického bezpečnostného incidentu a výsledok oznamuje Prevádzkovateľovi základnej služby. Prevádzkovateľ základnej služby sa zaväzuje bezodkladne informovať Zhotoviteľa o každom kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti Zhotoviteľa, o ktorých sa dozvie, a to spôsobom určeným touto Zmluvou. Prevádzkovateľ základnej služby určuje závažnosť kybernetického bezpečnostného incidentu a výsledok oznamuje Zhotoviteľovi. Zhotoviteľovi a Prevádzkovateľ základnej služby sa zaväzujú poskytnúť si vzájomnú súčinnosť pri riešení kybernetických bezpečnostných incidentov a skutočností majúcich vplyv na zabezpečenie kybernetickej bezpečnosti podľa tohto bodu Zmluvy.
7. Prevádzkovateľ kritickej základnej služby a Zhotoviteľ sa dohodli, že Zhotoviteľ je oprávnený podľa vlastného uváženia a na vlastnú zodpovednosť zapojiť ďalšieho zmluvného partnera (ďalej len „**subdodávateľ**“) úplne alebo čiastočne zabezpečujúceho alebo akýmkoľvek spôsobom sa podieľajúceho na službách pre Prevádzkovateľa základnej služby namiesto Zhotoviteľa alebo spolu s Zhotoviteľom. Zhotoviteľ sa zaväzuje, že nezapojí ďalšieho subdodávateľa predtým, než dostane písomný súhlas Prevádzkovateľa kritickej základnej služby.
8. Zoznam subdodávateľov tvorí prílohu hlavnej Zmluvy. Zhotoviteľ je plne zodpovedný voči Prevádzkovateľovi základnej služby za plnenie povinností subdodávateľa.
9. Zhotoviteľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby v zmysle komunikačnej matice o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Zhotoviteľom.

**Článok IV.**

**AUDIT KYBERNETICKEJ BEZPEČNOSTI /BEZPEČNOSTNÝ AUDIT**

1. Prevádzkovateľ základnej služby je oprávnený vykonať na dotknutom diele, v rámci ktorého sa nachádza kritická základná služba Prevádzkovateľ základnej služby voči Zhotoviteľovi ako aj u jeho subdodávateľov audit zameraný na overenie plnenia povinností podľa tejto Zmluvy KB, ZoKB a Vyhlášky o bezpečnostných opatrení a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Zhotoviteľa a subdodávateľov na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí.
2. Prevádzkovateľ základnej služby môže audit voči Zhotoviteľovi a subdodávateľom realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
3. Zhotoviteľ sa zaväzuje za seba ako aj za subdodávateľov pri audite spolupracovať s   
   Prevádzkovateľom základnej služby a sprístupniť mu priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
4. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Zhotoviteľa a subdodávateľom, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti a prevádzky systémov podľa hlavnej zmluvy a tejto Zmluvy KB.
5. V rámci auditu sú Zhotoviteľ a subdodávatelia povinní preukázať Prevádzkovateľovi základnej služby súlad s touto Zmluvou KB, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto Zmluvy KB a aktuálnosť svojej bezpečnostnej dokumentácie.
6. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Zhotoviteľovi najmenej 15 (pätnásť) pracovných dní vopred svoj zámer realizovať u Zhotoviteľa alebo jeho subdodávateľov audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezbavuje Zhotoviteľa zodpovednosti za plnenie povinností Zhotoviteľa vyplývajúcich z tejto Zmluvy KB. Ak Zhotoviteľ alebo jeho subdodávateľ neumožní vykonanie auditu, považuje sa to za podstatné porušenie Zmluvy KB a Prevádzkovateľ kritickej základnej služby je oprávnený vyvodiť voči Zhotoviteľa zmluvné sankcie.
7. Prípadné nedostatky zistené auditom sú Zhotoviteľ a subdodávatelia povinní odstrániť bez zbytočného odkladu. V prípade, že tieto nedostatky nebudú v  lehote 60 (šesťdesiat) dní od zistenia na základe auditu odstránené, považuje sa to za podstatné porušenie Zmluvy KB zo strany Zhotoviteľa.
8. Prevádzkovateľ základnej služby ako aj Zhotoviteľ a jeho subdodávateľ sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia o mlčanlivosti tejto Zmluvy KB sa uplatňujú primerane.
9. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Zhotoviteľa alebo jeho subdodávateľov v rámci výkonu auditu musia dodržiavať pokyny Zhotoviteľa alebo jeho subdodávateľov týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „**BOZP**")a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „**PO**"),s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Zhotoviteľa alebo jeho subdodávateľov na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Zhotoviteľ. Zhotoviteľ sa zaväzuje pred vykonaním auditu v priestoroch Zhotoviteľa alebo jeho subdodávateľov písomne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Zhotoviteľa alebo jeho subdodávateľov môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Zhotoviteľ alebo jeho subdodávatelia 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 Zhotoviteľa alebo jeho subdodávateľov.
10. Pre vylúčenie akýchkoľvek pochybností sa Zhotoviteľ zaväzuje zabezpečiť Prevádzkovateľovi základnej služby vykonanie auditu v zmysle tohto článku tejto Zmluvy KB aj u svojich subdodávateľov.

**Článok VI.**

**POSTUP PRI RIEŠENÍ KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV**

1. Zhotoviteľ sa zaväzuje bezodkladne hlásiť každý kybernetický bezpečnostný incident, ako aj všetky ďalšie informácie požadované Prevádzkovateľom základnej služby na plnenie jeho povinností vplývajúcich zo ZoKB a informácie majúce vplyv na Zmluvu KB ako aj hlavnú zmluvu Prevádzkovateľovi kritickej základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov. Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, Zhotoviteľ sa zaväzuje odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Zhotoviteľ sa po detekcii kybernetického bezpečnostného incidentu zaväzuje riešiť kybernetické bezpečnostné incidenty najmä odozvou alebo inou reakciou na kybernetický bezpečnostný incident, ohraničením kybernetického bezpečnostného incidentu a jeho dopadov, nápravou následkov kybernetického bezpečnostného incidentu, asistenciou pri riešení kybernetického bezpečnostného incidentu na mieste, reakciou na kybernetický bezpečnostný incident a podporou reakcií na kybernetický bezpečnostný incident (ďalej len „**reaktívne opatrenie**“).Pri riešení kybernetických bezpečnostných incidentov je Zhotoviteľ povinný na žiadosť Prevádzkovateľa kritickej základnej služby spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a ďalším ústredným orgánom alebo iným orgánom štátnej správy určeným v § 4 ZoKB jednať, a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy KB alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického bezpečnostného incidentu.
3. Zmluvné strany zabezpečia uchovanie relevantných údajov a materiálov potrebných na vyšetrovanie incidentu, pričom budú dodržiavať všetky platné právne predpisy.
4. Zhotoviteľ sa zaväzuje bezodkladne, najneskôr však do 24 (dvadsaťštyri) hodín po nasadení reaktívnych opatrení v zmysle bodu 2 tohto článku Zmluvy KB, oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia v súlade § 27 ods. 4 ZoKB vo formulári, ktorého vzor tvorí prílohu č. 4 tejto Zmluvy KB.
5. Po vyriešení kybernetického bezpečnostného incidentu je Zhotoviteľ na výzvu Prevádzkovateľa základnej služby povinný predložiť Prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického bezpečnostného incidentu (ďalej len „**ochranné opatrenia**“)na schválenie. Ak Zhotoviteľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Zhotoviteľ povinný spolupracovať s Prevádzkovateľom základnej služby na jeho návrhu.
6. Po schválení ochranného opatrenia Prevádzkovateľom základnej služby, je Zhotoviteľ povinný ochranné opatrenie bez zbytočného odkladu, najneskôr však v lehote vyplývajúcej z opatrení schválených príslušným odborom gestora IS, vykonať.Po vykonaní ochranného opatrenia Zhotoviteľom, je Zhotoviteľ povinný za prítomnosti MIKB Prevádzkovateľa základnej služby preveriť jeho efektívnu účinnosť. Zmluvné strany sa dohodli, že účinnosť ochranných opatrení bude podmienená výkonom penetračného testovania, pričom záver takéhoto testovania bude vyhodnotený na základe protokolu o efektívnom účinku ochranného opatrenia za Prevádzkovateľa kritickej základnej služby signovanom MIKB a za Zhotoviteľa signovanom osobou.
7. Náklady spojené s riešením bezpečnostného incidentu znáša Strana, ktorá je za incident priamo zodpovedná (napr. porušením zmluvy, nedbalosťou). Ak nie je možné jednoznačne určiť zodpovednosť, strany znášajú náklady spoločne podľa vopred dohodnutého pomeru.

**Článok VII.**

**ZÁVÄZOK MLČANLIVOSTI**

1. Zhotoviteľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením hlavnej zmluvy a tejto Zmluvy KB, 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. Zhotoviteľ je povinný chrániť najmä 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. Zhotoviteľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Zhotoviteľovi.
2. Zhotoviteľ sa v rovnakom rozsahu zaväzuje zaviazať povinnosťou mlčanlivosti aj všetky ním poverené osoby, ktoré budú zúčastnené na predmete plnenia tejto Zmluvy KB (t. j. jeho zamestnanci, subdodávatelia a ich zamestnanci). Zhotoviteľ je povinný na požiadanie preukázať Prevádzkovateľovi základnej služby splnenie tejto povinnosti. Povinnosť mlčanlivosti trvá aj po zániku ich pracovno-právneho vzťahu alebo obchodného vzťahu. Povinnosť zachovávať mlčanlivosť podľa tohto článku Zmluvy KB trvá aj po skončení tejto Zmluvy KB resp. hlavnej zmluvy. Mlčanlivosť sa vzťahuje na všetkých zástupcov Zhotoviteľa ako aj jeho Subdodávateľov.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje ZoKB.
4. Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa ZoKB nie je dotknutá povinnosť mlčanlivosti alebo zachovania obchodného tajomstva podľa osobitných predpisov.
5. Zmluvné strany sa dohodli, že všetky informácie, najmä technické údaje o dotknutých systémoch, projektové dokumentácie, technická dokumentácia, prihlasovacie údaje, administrátorské používateľské mená a heslá, prístupové a licenčné kľúče, overovacie kódy, master kódy, RFID zoznamy, prístupové karty a iné bezpečnostné informácie, sa považujú za dôverné informácie. Zhotoviteľ ako aj Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o týchto informáciách, neprenášať ich tretím stranám v čase trvania hlavnej zmluvy bez súhlasu a nepoužívať ich na iný účel, ako je plnenie tejto alebo hlavnej zmluvy. Tento záväzok platí počas trvania zmluvy aj po jej skončení mimo plnenia potrieb zabezpečenia ďalších zmluvných nových záväzkov súvisiacou s prevádzkou dotknutých systémov.
6. Prevádzkovateľ základnej služby sa zaväzuje uchovávať všetky odovzdané dôverné údaje v súlade s pravidlami informačnej bezpečnosti a zabezpečiť ich pred neoprávneným prístupom, stratou alebo zneužitím. Tieto údaje budú použité výhradne v krízovej situácii po písomnom informovaní Zhotoviteľa. Obe strany sa zaväzujú, že s týmito údajmi budú nakladať v súlade s platnými právnymi predpismi, najmä v súlade so zákonom o kybernetickej bezpečnosti a ochranou osobných údajov.

**Článok VIII.**

**Povinnosti po skončení Zmluvy**

* 1. Po ukončení tejto Zmluvy KB je Zhotoviteľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto Zmluvy KB prístup, resp. podľa písomného pokynu Prevádzkovateľa základnej služby zabezpečí preukázateľné zničenie akýchkoľvek nosičov elektronickej informácie certifikovanou organizáciu, a doložením protokolu s podpismi oprávnených osôb Zhotoviteľa a PZS.
  2. Zmluvné strany berú na vedomie, že predmetom plnenia hlavnej zmluvy môže byť autorské dielo podľa zákona č. 185/2015 Z. z. Autorský zákon v platnom znení, ktorého súčasťou môže byť:
     1. softvér, ktorý bol vytvorený Zhotoviteľom predovšetkým pre podmienky a potreby Prevádzkovateľa kritickej základnej služby;
     2. softvér Zhotoviteľa, ktorý má všeobecný charakter;
     3. softvér tretích osôb; alebo
     4. Open Source softvér, ktorý je podriadený príslušnej licencii slobodného softvéru.
  3. Zmluvné strany berú ďalej na vedomie, že predmetom plnenia hlavnej zmluvy môže byť aj vytvorenie alebo poskytnutie iných predmetov duševného vlastníctva, ako sú napr. technická a užívateľská dokumentácia, prevádzkový manuál, návrh riešenia k Softvéru alebo k Balíkovému softvéru alebo konkrétne digitálne dizajny, vrátane grafického užívateľského rozhrania (GUI), jednotlivých ikon či symbolov, prípadne konkrétne know-how Zhotoviteľa.
  4. S ohľadom na body 1, 2 a 3 tohto článku Zmluvy KB, zmluvné strany berú na vedomie, že Zhotoviteľ je v zmysle § 9 ods. 2 písm. p) Vyhlášky NBÚ povinný po zániku hlavnej zmluvy umožniť Prevádzkovateľovi základnej služby zabezpečiť kontinuitu prevádzkovanej základnej služby vo vzťahu k službám, ktoré priamo súvisia s prevádzkou tejto základnej služby v rámci sietí a informačných systémov Prevádzkovateľa základnej služby.
  5. Ustanovenie bodov 1 až 3 tohto článku Zmluvy KB sa uplatňuje pre dodávku autorského diela v opačnom prípade sa neaplikuje.
  6. Všetky ostatné licenčné podmienky sa riadia hlavnou zmluvou.

**Článok IX.**

**Zodpovednosť za škodu**

* 1. Zmluvné strany zodpovedajú za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinnosti zmluvnej strany stanovenej ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvou KB.
  2. V prípade, ak v dôsledku porušenia ZoKB alebo preukázateľného porušenia povinností vyplývajúcich z tejto Zmluvy KB na strane Zhotoviteľa alebo jeho subdodávateľov v rozsahu povinností Zhotoviteľa vyplývajúcich z tejto zmluvy a vznikne Prevádzkovateľovi základnej služby ujma alebo finančná sankcia, Zhotoviteľ zodpovedá za spôsobenú škodu podľa ustanovení ZoKB. V prípade sankcie uloženej Národným bezpečnostným úradom, túto znáša v plnom rozsahu Zhotoviteľ, výlučne v prípade priameho dokázania porušenia nezávislou treťou stranou voči Prevádzkovateľovi základnej služby a Zhotoviteľovi.
  3. V prípade, že zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvy KB (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.
  4. Vznik zodpovednosti porušujúcej zmluvnej strany za škodu vzniknutú poškodenej zmluvnej strane je však podmienená povinnosťou poškodenej zmluvnej strany preukázať porušujúcej zmluvnej strane existenciu príčinnej súvislosti medzi porušením povinnosti podľa Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy na strane porušujúcej zmluvnej strany a vznikom škody. Príčinná súvislosť je okrem iného daná aj vtedy, ak porušujúca zmluvná strana nesplnila svoju všeobecnú preventívnu povinnosť počínať si tak, aby nedochádzalo ku vzniku škôd. Počínaním podľa predchádzajúcej vety sa rozumie najmä akýkoľvek postup zmluvnej strany, na ktorý je v zmysle Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy oprávnená a prostredníctvom ktorého mohlo byť vzniku škody zabránené.
  5. V prípade preukázania existencie príčinnej súvislosti podľa tohto článku Zmluvy KB je porušujúca zmluvná strana povinná uhradiť poškodenej zmluvnej strane vzniknutú škodu, a to v lehote do 30 (tridsať) dní odo dňa doručenia písomnej výzvy porušujúcej zmluvnej strane na adresu uvedenú v záhlaví tejto Zmluvy KB. V prípade potreby vzniknutú škodu posúdi nezávislá tretia strana, ktorú zabezpečí Prevádzkovateľ kritickej základnej služby.
  6. Zánikom tejto Zmluvy KB nie sú dotknuté tie ustanovenia, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zániku tejto Zmluvy KB a záväzky na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy KB.

**Článok X.**

**KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI**

1. Zhotoviteľ sa zaväzuje komunikovať pri plnení povinností podľa tejto Zmluvy KB   
   s Prevádzkovateľom základnej služby spôsobom určeným Prevádzkovateľom základnej služby, t.j. v zmysle komunikačnej matice. Zhotoviteľ je povinný zabezpečiť technické a organizačné podmienky na zabezpečený (šifrovaný) prenos informácií, napríklad prostredníctvom PGP šifrovania alebo šifrovaním príloh formou ZIP ( AES-256), a to najmä pri komunikácii týkajúcej sa citlivých záležitostí, ako je riešenie bezpečnostných incidentov alebo poskytovanie podkladov obsahujúcich chránené informácie podľa klasifikácie informácií Prevádzkovateľa základnej služby.
2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Zhotoviteľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.
3. Zhotoviteľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.
4. Kontaktné osoby podľa prílohy č. 1 tejto Zmluvy KB môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia Zmluvy KB o doručovaní.

**Článok XI.**

**SPOLOČNÉ USTANOVENIA**

1. Zhotoviteľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB v súlade so ZoKB a jeho vykonávacími predpismi ostatnej platnej legislatívy, 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.
2. Zhotoviteľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na kritickú základnú službu Prevádzkovateľa kritickej základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa kritickej základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Zhotoviteľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy KB na zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
4. Zhotoviteľ sa zaväzuje dokumentovať svoju činnosť podľa tejto Zmluvy KB..
5. Zhotoviteľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB bezodkladne odo dňa začiatku skúšobnej prevádzky bez účasti verejnosti v rámci objektov a systémov súvisiacich s dotknutou základnou službou, pokiaľ to nie je v tejto Zmluve KB alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak. ( Požiadavka sa týka výlučne nových stavebných objektov)
6. V prípade, ak Zhotoviteľ plní Zmluvu KB prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby, Zhotoviteľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto Zmluvy KB aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto Zmluvy KB. Zhotoviteľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto Zmluvy KB aj u týchto subdodávateľov.
7. Akékoľvek oznámenia zmluvných strán podľa tejto Zmluvy KB realizované formou e-mailu sa považujú za doručené druhej zmluvnej strane nasledujúci pracovný deň po dni, kedy bolo odosielateľovi preukázateľne odoslané potvrdenie o doručení e-mailu adresátovi bez ohľadu na to, či došlo k prečítaniu správy na strane adresáta, s tým, že v prípade detekcie kybernetického bezpečnostného incidentu a povinností Zhotoviteľa spojených s jeho hlásením Prevádzkovateľovi základnej služby je podmienené aj odoslaním SMS MIKB podľa ustanovenia článku VI bod 2 Zmluvy KB.
8. V prípade ak Zhotoviteľ bude na základe vlastnej žiadosti zaradený Národným bezpečnostným úradom ako Prevádzkovateľ základnej služby, prípadne Prevádzkovateľ kritickej základnej služby do registra prevádzkovateľov základnej služby v zmysle zákona o kybernetickej bezpečnosti je povinný informovať o tejto skutočnosti Prevádzkovateľa kritickej základnej služby, najneskôr do pätnásť (15) Dní odo dňa zaradenia, ak v tejto súvislosti nie je v súlade so hlavnou zmluvou stanovená iná lehota.
9. Prevádzkovateľ identifikoval Zhotoviteľa akou treťou stranou podľa § 19 ods. 2 ZoKB. Zhotoviteľ má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti prevádzkovanej kritickej základnej služby. Z uvedeného dôvodu je Zhotoviteľ povinný sa dňom účinnosti tejto zmluvy riadiť ZoKB a splniť si povinnosti ako identifikovaná Tretia strana, a nahlásiť sa Národnému bezpečnostnému úradu v zmysle lehôt stanovených v ZoKB.
10. Zhotoviteľ je povinný do 15 pracovných dní od doručenia Potvrdenia o zaradení do registra prevádzkovateľov základných služieb z Národného bezpečnostného úradu o tejto skutočnosti písomné informovať Prevádzkovateľa základnej služby.
11. Pojmy uvedené v tejto Zmluve sa zhodujú s pojmami definovanými ZoKB a v prípade ich slovnej nezhody sa použijú ustanovenia ZoKB, ktoré sú im významom najbližšie.
12. Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia ZoKB a ostatnými príslušnými právnymi predpismi.

# Článok XII.

# Vyššia moc

1.Vyššia moc znamená mimoriadnu udalosť alebo okolnosť, ktorú nemohla žiadna zo zmluvných strán pred uzatvorením Zmluvy KB predvídať, ktorá je mimo kontroly ktorejkoľvek zo zmluvných strán a nebola spôsobená úmyselne alebo z nedbanlivosti konaním alebo opomenutím ktorejkoľvek zmluvnej strany a ktorá podstatným spôsobom sťažuje alebo znemožňuje plnenie povinností podľa Zmluvy KB ktoroukoľvek zo zmluvných strán. Takýmito udalosťami alebo okolnosťami sú najmä živelné pohromy alebo prírodné katastrofy. Výslovne sa stanovuje, že vyššou mocou nie je štrajk personálu Zhotoviteľa ani hospodárske pomery zmluvných strán ( tzn. finančnú a ekonomickú situáciu jednotlivých zmluvných strán). .

2. Ak niektorej zo zmluvných strán bráni alebo bude brániť v plnení niektorej jej povinnosti podľa Zmluvy KB vyššia moc, potom písomne oznámi druhej zmluvnej strane udalosť alebo okolnosti, ktoré predstavujú vyššiu moc, uvedie povinnosti, v ktorých plnení jej vyššia moc bráni alebo bude brániť a predpokladané trvanie takej okolnosti predstavujúcej vyššiu moc. Oznámenie musí byť urobené bezodkladne, najneskôr však v lehote 15 (pätnásť) dní potom, čo sa zmluvná strana dozvedela alebo sa pri vynaložení riadnej odbornej starostlivosti mala a mohla dozvedieť o príslušnej udalosti alebo okolnostiach predstavujúcich dôvod vyššej moci. Ak je to možné, pri vynaložení riadnej odbornej starostlivosti, musí uvedené oznámenie obsahovať návrh opatrení vedúcich k zmierneniu alebo vylúčeniu dôsledkov okolností predstavujúcich vyššiu moc. V ostatných prípadoch bude oznámenie obsahovať iba najbližší možný termín, do ktorého môže byť návrh opatrenia poskytnutý pri vynaložení primeraného úsilia. Ak návrh opatrenia druhá zmluvná strana schváli, na čo má lehotu 15 (pätnásť) dní, postupuje zmluvná strana dotknutá vyššou mocou podľa neho až do ukončenia okolností vyššej moci.

3. Po uskutočnení tohto oznámenia príslušnou zmluvnou stranou, nebude táto zmluvná strana zodpovedná za príslušné porušenia  povinností po dobu, dokiaľ jej vyššia moc bráni alebo bude brániť v ich plnení.

4. Zmluvnú stranu nezbavuje zodpovednosti za porušenie povinnosti vyššia moc, ktorá nastala až v čase, kedy bola povinná zmluvná strana v omeškaní s plnením jej povinnosti. Účinky vylúčenia zodpovednosti sú obmedzené iba na dobu, dokiaľ trvá vyššia moc.

5. Každá zmluvná strana vždy vyvinie všetko úsilie potrebné k tomu, aby minimalizovala omeškanie pri plnení svojich povinností podľa Zmluvy KB , ktoré vzniklo v dôsledku vyššej moci, najmä plniť návrh opatrenia, ak je tento schválený druhou zmluvnou stranou.

6. Príslušná zmluvná strana oznámi druhej zmluvnej strane okamih ukončenia pôsobenia vyššej moci v rovnakej lehote ako pri oznámení o jej vzniku podľa bodu 2 tohto článku tejto Zmluvy KB.

7. Ak je z dôvodu okolnosti vylučujúcej zodpovednosť alebo prípadu vyššej moci plnenie Zmluvy KB jednej zo zmluvných strán ovplyvnené len čiastočne, takáto zmluvná strana zostáva zodpovedná za plnenie tých záväzkov, ktoré okolnosťou vylučujúcou zodpovednosť alebo vyššou mocou nie sú dotknuté.

8. Ak má niektorý zo subdodávateľov podľa akejkoľvek zmluvy či dohody týkajúcej sa poskytovania služby podľa tejto Zmluvy KB širšie definovaný nárok na omeškanie v dôsledku pôsobenia vyššej moci, okolností vylučujúcich zodpovednosť alebo iného obdobného právneho inštitútu, než ako je definovaná vyššia moc podľa tejto Zmluvy KB, takéto širšie definované udalosti alebo okolnosti neospravedlňujú porušenie povinností podľa Zmluvy KB s Zhotoviteľom ani mu nezakladajú nároky podľa tohto článku Zmluvy KB.

**Článok XIV.**

**SANKCIE**

1. Zmluvné strany sa dohodli, že v prípade porušenia ktorejkoľvek povinnosti Poskytovateľa uvedenej v bodoch Prílohy č. 2 tejto Zmluvy je PZS oprávnený uložiť Poskytovateľovi zmluvnú pokutu vo výške 500 EUR ( slovom: päťsto eur) za každý, aj začatí deň trvania porušenia povinnosti, až do vykonania nápravy, a to aj opakovane a za každé jednotlivé porušenie povinnosti samostatne.

2. V prípade, ak Zhotoviteľ spôsobí Prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo Zmluvy KB akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. Pre odstránenie právnych pochybností, zodpovednosť Zhotoviteľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Zhotoviteľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Zhotoviteľom.

1. Zmluvné strany sa dohodli, že v prípade, ak dôjde k porušeniu povinností vyplývajúcich zo ZoKB alebo tejto Zmluvy zo strany Prevádzkovateľa základnej služby, a v dôsledku tohto porušenia vznikne Zhotoviteľovi preukázateľná škoda, Prevádzkovateľ základnej služby zodpovedá za túto škodu podľa § 373 a nasl. Obchodného zákonníka. Zodpovednosť Prevádzkovateľa základnej služby nevzniká v prípade, ak bolo porušenie spôsobené prekážkou, ktorú nemohol pri vynaložení odbornej starostlivosti predvídať ani odvrátiť, alebo ak nebolo možné plnenie požiadaviek z dôvodu preukázateľne nepriaznivých hospodárskych pomerov Prevádzkovateľa základnej služby, o ktorých bol Zhotoviteľ riadne a včas informovaný.
2. Zmluvné strany sa dohodli, že uplatnením sankcií v zmysle tohto článku Zmluvy KB nie je dotknutý nárok Prevádzkovateľa základnej služby na náhradu škody, ktorá mu vznikla porušením povinností Zhotoviteľa.
3. Zaplatenie zmluvnej pokuty nezbavuje Zhotoviteľa povinnosti splniť záväzok zabezpečený zmluvnou pokutou.

**Článok XV.**

**TRVANIE ZMLUVY**

1. Táto Zmluva KB sa uzatvára na dobu určitú, a to na dobu trvania hlavnej zmluvy. Táto Zmluva KB môže byť ukončená v prípadoch ustanovených v Zmluve KB alebo na základe zákona.
2. Za podstatné porušenie Zmluvy KB sa považuje:
3. porušenie ktorejkoľvek povinnosti uvedenej v tejto Zmluvy KB;
4. ak Zhotoviteľ, ako strana porušujúca Zmluvu KB, vedel v čase uzavretia Zmluvy KB alebo v tomto čase bolo rozumné predvídať s prihliadnutím na účel Zmluvy KB, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola Zmluva KB uzavretá, že Prevádzkovateľ základnej služby nebude mať záujem na plnení povinností pri takom porušení Zmluvy KB;
5. Zhotoviteľ neposkytne potrebnú súčinnosť v zmysle tejto Zmluvy KB.
6. Odstúpením/okamžitým odstúpením od hlavnej zmluvy Zmluva KB zaniká.
7. Túto Zmluvu KB nie je možné vypovedať Zhotoviteľom ani Prevádzkovateľom základnej služby, a je viazaná na účinnosť hlavnej zmluvy.

**Článok XVI.**

**ZÁVEREČNÉ USTANOVENIA**

* 1. Táto Zmluva KB sa spravuje zákonmi Slovenskej republiky. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
  2. Prípadné spory vyplývajúce z tejto Zmluvy KB budú riešené predovšetkým mimosúdne. Podpisom tejto Zmluvy KB zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto Zmluvy KB sú príslušné súdy Slovenskej republiky.
  3. Táto Zmluva KB sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo Zmluvy KB nevyplýva niečo iné.
  4. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto Zmluvy KB na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
  5. V prípade, ak niektoré z ustanovení Zmluvy KB je alebo sa stane neúplným, neplatným, neúčinným a/alebo nevykonateľným, nie sú tým dotknuté ostatné ustanovenia Zmluvy KB, pokiaľ z jeho povahy, obsahu alebo okolností, za ktorých bolo dojednané nevyplýva, že ho nie je možné oddeliť od ostatného obsahu Zmluvy KB. Zmluvné strany sa zaväzujú bez zbytočného odkladu nahradiť takéto neúplné, neplatné, neúčinné a/alebo nevykonateľné ustanovenie, takým úplným, platným, účinným a/alebo vykonateľným ustanovením, ktoré svojím obsahom najviac zodpovedá nahrádzanému ustanoveniu.
  6. Táto Zmluva KB predstavuje úplnú dohodu zmluvných strán o jej obsahu. Podpisom tejto Zmluvy KB zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto Zmluvy KB a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto Zmluve KB neuvedených, ústnych alebo písomných dojednaní a dohôd.
  7. Táto Zmluva KB bola vyhotovená v **(4) štyroch** rovnopisoch, po (2) dvoch pre každú zmluvnú stranu.
  8. Zmluvné strany berú na vedomie, že Prevádzkovateľ základnej služby je v zmysle § 2 ods. 1 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 zmluva v zmysle § 5a tohto zákona v spojení s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov povinne zverejňovanou zmluvou.
  9. Táto Zmluva KB nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv.
  10. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
* Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa kritickej základnej služby a Zhotoviteľa - **nezverejňuje sa v CRZ**
* Príloha č. 2 - Špecifikácia a rozsah bezpečnostných opatrení - **nezverejňuje sa v CRZ**
  1. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto Zmluvu KB neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy KB dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

|  |  |  |
| --- | --- | --- |
| **Prevádzkovateľ základnej služby**: |  | **Zhotoviteľ:** |

V Bratislave dňa..... V ......... dňa .....

Odtlačok pečiatky Odtlačok pečiatky

**....................................... ............................................**

**Ing. Filip Macháček Doplniť**

predseda predstavenstva predseda predstavenstva/ vedúci člen

a generálny riaditeľ

**........................................ .............................................**

**Ing. Július Mihálik Doplniť**

člen predstavenstva člen

**Príloha č. 1:** Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Zhotoviteľa

Prevádzkovateľ základnej služby:

|  |  |  |  |
| --- | --- | --- | --- |
| **Meno a priezvisko** | **Rola** | **Telefónny kontakt** | **Email** |
|  | Manažér informačnej a kybernetickej bezpečnosti |  |  |
|  | Vedúca oddelenia riadenia IB a KB |  |  |
|  | Gestor základnej služby |  |  |

Zhotoviteľ:

|  |  |  |  |
| --- | --- | --- | --- |
| **Meno a priezvisko** | **Rola** | **Telefónny kontakt** | **Email** |
|  | Kontaktná osoba pre oblasť informačnej a kybernetickej bezpečnosti |  |  |
|  | Projektový manažér |  |  |
|  | Osoba zodpovedná za poskytnutie služby |  |  |
|  | Osoba zodpovedná za poskytnutie služby |  |  |
|  | + Kompletný zoznam Programátorov a osôb spravujúcich dotknuté systémy – aj všetci subdodávatelia |  |  |

**Príloha č. 2 Špecifikácia a rozsah bezpečnostných opatrení**

Plnením bezpečnostných opatrení a všetkých činností v zmysle zákona č. 69/2018 Z.z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej ako „Zákon o kybernetickej bezpečnosti“ v príslušnom gramatickom tvare) sa rozumejú činnosti nad prostredím prevádzkovanej základnej služby „Centrálny riadiaci systém tunelov“ a „Informačný systém diaľnic a rýchlostných ciest“, a nejedná sa o interné prostredie Zhotoviteľa. Požadované plnenie politík a postupov sa taktiež týka výhradne dotknutých prevádzkovaných kritických základných služieb.

1. **Bezpečnostné opatrenia pre organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti**:
   1. určiť na strane Zhotoviteľa zodpovednú osobu za kybernetickú bezpečnosť a plnenie
   2. mať na strane Zhotoviteľa zavedený systém vzdelávania a preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti.
   3. Zhotoviteľ je povinný zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Zhotoviteľa a jeho subdodávateľov nebolo možné zasiahnuť siete a informačné systémy PZS,
   4. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy KB alebo budú mať prístup k PZS,
   5. Zhotoviteľ je povinný uplatňovať zásadu sprístupňovania informácií podľa zásady aktuálnej potreby poznať, podľa ktorej prístup k informáciám a ich vlastníctvo je obmedzené len na tie osoby, ktoré z dôvodu plnenia svojich úloh alebo povinností musia byť s takýmito informáciami oboznámené alebo ich spracúvajú.)
   6. kópia hesiel k privilegovaným účtov (t.z. k účtom s najvyššími oprávneniami systémov) bude uložená v zabezpečenej forme schválenej Manažérom informačnej a kybernetickej bezpečnosti PZS v zabezpečenom priestore Zhotoviteľa. V prípade potreby prístupu k uvedenej kópii generických hesiel privilegovaných účtov, musí byť o prístupe a ich použití informovaný Manažér informačnej a kybernetickej bezpečnosti PZS najneskôr do 24 hodín, v prípade využitia v priebehu nepracovného dňa, je povinný Zhotoviteľ informovať o tejto skutočnosť Manažéra informačnej a kybernetickej bezpečnosti PZS prostredníctvom elektronickej komunikácie.

1. **Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb:**
   1. implementácia nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
   2. implementácia nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
   3. využívanie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov,
   4. Zhotoviteľ je povinný vykonávať pravidelné bezpečnostné kontroly zamerané na detekciu existujúcich zraniteľností v sieťových aktívach. Tieto kontroly sa budú vykonávať minimálne raz za 12 mesiacov pre všetky určené sieťové komponenty. Určené kritické aktíva budú definované na základe ich dôležitosti pre prevádzku a bezpečnosť systému. V prípade identifikácie zraniteľností je Zhotoviteľ povinný bezodkladne prijať primerané opatrenia na ich odstránenie alebo zmiernenie rizík,
   5. v prípade identifikácie zraniteľností s CVSS 3.0 vyšším ako hodnota 7.0, Zhotoviteľ poskytne PZS zoznam týchto identifikovaných zraniteľností aj s určením dotknutých aktív,
   6. Zhotoviteľ zabezpečí identifikáciu potrieb softvérových záplat a aktualizácií, ako aj zabezpečuje ich implementáciu na základe posúdenia rizík a analýzy vplyvov ,
   7. Ak Zhotoviteľ identifikuje zraniteľnosť, ktorá môže mať dopad na prevádzku alebo bezpečnosť systémov PZS, je povinný postupovať podľa § 24 zákona č. 69/2018 Z. z. a bezodkladne túto skutočnosť oznámiť PZS s informáciou o charaktere zraniteľnosti, dotknutých aktívach a navrhovaných opatreniach na jej odstránenie alebo zmiernenie rizík.
   8. zabezpečiť pravidelnú údržbu a aktualizácie technických zariadení a softvérov,
   9. vzor formuláru na nahlasovanie zraniteľností a kybernetických hrozieb Zhotoviteľovi poskytne PZS do 14 pracovných dní od účinnosti tejto zmluvy.
2. **Bezpečnostné opatrenia pre správu aktív a riadenie kybernetických hrozieb a rizík formou opatrení:**
   * + 1. Zhotoviteľ je povinný zabezpečiť, že jeho zamestnanci pri zmene alebo pri ukončení pracovného pomeru, zmluvy alebo obdobného zmluvného vzťahu preukázateľným spôsobom mu vracajú všetky aktíva PZS, ktoré mali zverené.

odovzdanie evidencie aktív a komponentov vo formáte dohodnutom s PZS, aktualizácia evidencie aspoň raz do roka a poskytnutie aktuálnej evidencie na vyzvanie PZS,

* 1. poskytnutie súčinnosti pri technickom vykonávaní kompletnej inventarizácie všetkých aktív v čase trvania Zmluvy aspoň raz ročne na vyzvanie PZS,
  2. Zhotoviteľ musí v prípade rozhodnutia PZS a pretrvávajúceho identifikovaného rizika, ktoré nie je možné mitigovať inou formou, prispôsobiť opatrenia na základe spätnej väzby od PZS a výsledkov hodnotení rizík v súlade s postupmi pre zmenové požiadavky definovanými hlavnou zmenou.
  3. Zhotoviteľ je povinný poskytnúť súčinnosť PZS pri revidovaní a aktualizovaní opatrení na riadenie rizík a ochranu aktív v súlade so zmenami v prostredí a novými hrozbami minimálne raz ročne.

1. **Bezpečnostné opatrenia pre riadenie udalostí a kybernetických bezpečnostných incidentov formou opatrení:**
   1. oboznámenie sa s postupmi PZS pri riešení KBI a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú minimálne postupy hlásenia KBI voči PZS,
   2. zabezpečiť plánovanie a testovanie riešenia kybernetických bezpečnostných incidentov aspoň raz za kalendárny rok spoločne s PZS a mať zadefinované, prijaté a oznámené procesy, úlohy a zodpovednosti v oblasti riešenia kybernetických bezpečnostných incidentov pri prevádzke dotknutých systémov,
   3. zabezpečovať posúdenie udalostí kybernetickej bezpečnosti a určenie ich priorít v prípade výskytu,
   4. je povinný mať definovaný systém reakcie na kybernetické bezpečnostné incidenty a poznatky získané z riešených kybernetických bezpečnostných incidentov sú preukázateľne zohľadnené v procese riadenia kybernetickej bezpečnosti,
   5. je povinný mať zavedené postupy na identifikáciu, zhromažďovanie, získavanie a uchovávanie digitálnych stôp súvisiacich s kybernetickými bezpečnostnými incidentmi,
   6. v prípade kybernetického bezpečnostného incidentu sú dodržiavané všetky stanovené bezpečnostné opatrenia a postupy,
   7. Zhotoviteľ je povinný pravidelne, aspoň raz ročne testovať pravidlá pre izoláciu kritických komponentov sietí, informačných systémov a operačných technológií počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotoví záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu, t.j. minimálne na dobu 2 rokov. Kópiu záznamu poskytne Zhotoviteľ na vyžiadanie PZS.
   8. Zhotoviteľ je povinný zabezpečiť riadenie a evidenciu odvrátených udalostí v súlade s požiadavkami vyhlášky č. 226/2025 Z. z. a zákona č. 69/2018 Z. z. Zhotoviteľ bezodkladne analyzuje každú odvrátenú udalosť s cieľom identifikovať jej príčinu, rozsah a dopad na bezpečnosť prevádzky informačných systémov PZS spadajúcich pod hlavnú zmluvu. O každej odvrátenej udalosti, ktorá by mohla viesť k vzniku kybernetického bezpečnostného incidentu alebo k narušeniu dostupnosti, integrity, dôvernosti alebo autenticity informačných aktív, je Zhotoviteľ povinný bezodkladne informovať PZS, a to najneskôr do 24 hodín od jej zistenia na email [MIKB@ndsas.sk](mailto:MIKB@ndsas.sk) a [ORB@ndsas.sk](mailto:ORB@ndsas.sk).
   9. Zhotoviteľ zabezpečí do 14 pracovaných dní od inštalácie bezpečnostných nástrojov pridelenie prístupov k výstupom z bezpečnostných nástrojov pre vopred určených zástupcov PZS z úseku bezpečnosti ako aj vstupné preškolenie všetkých určených zamestnancov PZS, ktorým budú sprístupnené výstupy z bezpečnostných nástrojov.
   10. riešenie zistených KBI a zníženie následkov zistených KBI podľa postupov PZS a prípadných doplňujúcich pokynov PZS,
   11. vyhodnocovanie spôsobov riešenia KBI po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI v súčinnosti s PZS,
   12. hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedenými v Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností a postupom a cez kontakty pre riešenie bezpečnostných incidentov uvedených v „Poriadku o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“. ,
   13. v prípade KBI Zhotoviteľ je povinný využívať aj formu hlásenia bezpečnostné incidentu, ktorá sa bude riadiť platnou bezpečnostnou politikou PZS – „Poriadok o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“.
   14. Zhotoviteľ je povinný zabezpečiť aktívnu pohotovosť pre riešenie bezpečnostných a prevádzkových incidentov. Na základe požiadavky Objednávateľa je Zhotoviteľ povinný nastúpiť k odstraňovaniu incidentu najneskôr do 3 hodín od doručenia výzvy alebo oznámenia incidentu prostredníctvom dohodnutého komunikačného kanála. Nesplnenie tejto lehoty sa považuje PZS za porušenie podmienok aktívnej pohotovosti a môže byť predmetom uplatnenia zmluvných sankcií podľa osobitných ustanovení tejto zmluvy. Povinnosť nastúpiť zahŕňa:
   15. zabezpečenie prítomnosti kvalifikovanej osoby schopnej začať s riešením incidentu (na mieste alebo vzdialene),
   16. potvrdenie prijatia výzvy a začiatku činnosti,
   17. a priebežnú komunikáciu o stave riešenia incidentu s určeným zástupcom PZS.
   18. Povinnosť nastúpiť do 3 hodín sa vzťahuje na kritické incidenty, ktoré majú alebo môžu mať vplyv na dostupnosť, integritu alebo bezpečnosť prevádzkovaných systémov. Kritickosť incidentu určuje PZS.
2. **Bezpečnostné opatrenia pre riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie**
   1. Zhotoviteľ je povinný aspoň raz ročne testovať záložné kópie dát, softvéru a konfigurácie sietí, informačných systémov a operačných technológií, o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu t.j. minimálne na dobu 2 rokov. Kópiu záznamu poskytne Zhotoviteľ na vyžiadanie PZS.
   2. Zálohy týkajúce sa operačných technológií sú oddelené v samostatnom zálohovacom systéme a minimálne raz ročne Zhotoviteľ vykonáva kontrolu funkčnosti záloh aspoň dvoch rôznych systémov; o kontrole funkčnosti záloh sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu, t.j. minimálne na dobu 2 rokov. Kópiu záznamu poskytne Zhotoviteľ na vyžiadanie PZS.
   3. Zhotoviteľ sa zaväzuje, počas trvania hlavnej zmluvy, najneskôr do troch (3) pracovných dní od zmeny údajov, PZS odovzdať v zalepenej zapečatenej obálke všetky prihlasovacie údaje (administrátorské užívateľské meno a heslo) do príslušného informačného systému na ich správu, prístupové licenčné kľúče, overovacie kľúče, prístupové master kódy do všetkých technických objektov a HW zariadení, zoznamy prístupových kariet, zoznamy pridelených RFID k zariadeniam z RFID čipom, zoznamy pridelených kľúčov od miestností vo vlastníctve PZS ako aj všetky ďalšie súvisiace prístupy. Zoznamy budú v tlačenej alebo elektronickej forme, ku každému prístupu bude uvedené okrem identifikácie prístupu aj meno prideleného, pracovné zaradenie, kontakt (mobil/e-mail), užívateľské meno, heslo. Prevádzkovateľ sa zaväzuje, že dané údaje budú uložené na bezpečnom mieste u MIKB PZS, a budú využité výhradne v krízovej situácii po písomnom informovaní Zhotoviteľa Prevádzkovateľom základnej služby.
   4. Zhotoviteľ sa zaväzuje, po skončení trvania hlavnej zmluvy, najneskôr do troch (3) pracovných dní PZS odovzdať všetky prihlasovacie údaje (administrátorské užívateľské meno a heslo) do príslušného informačného systému na ich správu, prístupové licenčné kľúče, overovacie kľúče, prístupové master kódy do všetkých technických objektov a HW zariadení, pridelené prístupové karty, zariadenia s RFID čipom, kľúče od miestností vo vlastníctve PZS, ako aj všetky ďalšie súvisiace prístupy pre zabezpečenie funkčného a bezproblémového prevzatia systémov a zachovania kontinuity činnosti.
3. **Bezpečnostné opatrenia pre bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií**
4. sú odinštalované alebo zakázané služby neslúžiace na vykonávanie činností pre PZS na podporných aktívach[[1]](#footnote-1)
5. komponenty operačných technológií sú konfigurované podľa odporúčaných bezpečnostných nastavení uvedených dodávateľom komponentu operačných technológií,
6. komponenty operačných technológií poskytujú rozhranie na prístup k aktuálne nasadeným bezpečnostným konfiguračným nastaveniam,
7. aspoň raz ročne Zhotoviteľ vykonávaná kontrolu a aktualizáciu konfigurácie komponentov sietí, informačných systémov a operačných technológií podľa vývoja hrozieb; o kontrole sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu, t.j. minimálne na dobu 2 rokov. Kópiu záznamu poskytne Zhotoviteľ na vyžiadanie PZS.
8. riadiaci systém umožňuje zabráneniu ďalšieho prístupu spustením uzamknutia relácie po konfigurovateľnom čase nečinnosti alebo manuálnym uzamknutím; blokovanie relácie zostáva v platnosti, ak používateľ, ktorý reláciu vlastní, alebo iný oprávnený používateľ neobnoví prístup pomocou schválených identifikačných a autentifikačných postupov. Toto opatrenie je relevantné pre komponenty zaradené do vrstiev pre operačné technológie 3 a vyššie[[2]](#footnote-2).
9. v rámci životného cyklu vývoja operačných technológií sú návrhy a zmeny vykonané vo vyhradenom vývojovom prostredí Zhotoviteľa,
10. Technické riešenie systému CRS ako aj jeho príslušné komponenty musia obsahovať:
    1. funkciu „mirroring“ (zrkadlenie portov LAN komunikačných komponentov) pre nasadenie zariadení pre potreby NDS (viď NDS box),
    2. „konektivitu“ pre zabezpečenú komunikáciu (IPsec, OpenVPN, ...)
11. **Bezpečnostné opatrenia pre bezpečnosť a spôsobilosti ľudských zdrojov / správu identít a prístupov**
12. Pri výkone práce na diaľku je Zhotoviteľ povinný využívať viacfaktorové overovanie pre vzdialený prístup; vzdialený prístup Zhotoviteľa a jeho subdodávateľov v zmysle hlavnej zmluvy do dotknutých informačných systémov musí byť schválený PZS v zmysle vopred definovaných postupov,
13. v prípade mimoriadnej situácie, napr. pri zásahu pri bezpečnostnom incidente, alebo pri prevádzkovom incidente, môže byť vzdialený prístup schválený dodatočne najneskôr nasledujúci pracovný deň,
14. prideľovať a odoberať prístupy iba na základe požiadavky gestora prevádzkovanej základnej služby, alebo ním určenej oprávnenej osoby,
15. v prípade potreby poskytnutie súčinnosti pri aktualizácií Evidencie prístupov, ktorú vedie PZS, na základe podkladov od Zhotoviteľa,
16. pri prideľovaní prístupov zástupcom Zhotoviteľa dodržiavať princíp najnižšieho oprávnenia, a to aby používatelia mali prístup len k tým systémom a dátam, ktoré sú nevyhnutné pre plnenie ich pracovných úloh a dodržiavať a vymedzenie príslušných zodpovedností používateľov a rolí.
17. zabezpečiť logovanie aktivít, a to všetkých prístupov a aktivít používateľov v systéme,
18. Zhotoviteľ je povinný zabezpečiť, aby do systému alebo siete mali prístup len technické prostriedky (zariadenia) a používatelia, ktorých oprávnenosť bola pred prístupom jednoznačne identifikovaná a overená. Oprávnenosť zariadenia a používateľa musí byť preukázateľne zdokumentovaná a riadená podľa zásady minimálnych oprávnení. Toto opatrenie je relevantné pre komponenty zaradené do vrstiev pre operačné technológie 3 a vyššie.
19. v prípade prístupu na inžinierske prostredia v rámci prostredia operačných technológií je zaistený prístup a overenie technológiou pre záznam a archiváciu úkonov Zhotoviteľa;
20. Zoznam pracovných rolí Zhotoviteľa a zoznam jeho zamestnancov a zamestnancov subdodávateľov, ktorí sa budú podieľať na plnení hlavnej zmluvy a tejto Zmluvy KB a/alebo budú mať prístup k informáciám a údajom PZS, je uvedený v prílohe č. 1 tejto Zmluvy KB a v hlavnej zmluve. Zhotoviteľ je povinný bezodkladne písomne oznámiť PZS každú zmenu v personálnom obsadení. Na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB.
21. Zhotoviteľ je povinný zaviazať povinnosťou mlčanlivosti podľa ZoKB osoby, ktoré sa budú podieľať na plnení Zmluvy KB ako aj hlavnej zmluvy.
22. **Bezpečnostné opatrenia pre bezpečnosť pri prevádzke sietí a informačných systémov:**
23. prevádzkové postupy pre zariadenia na spracovanie informácií, siete a informačné systémy sú zdokumentované a sprístupnené zamestnancom PZS podľa ich potreby a sú vždy aktuálne,
24. Zhotoviteľ pri plnení predmetu hlavnej Zmluvy zabraňuje strate, poškodeniu, krádeži alebo kompromitácii aktív alebo prerušeniu prevádzky v súvislosti s narušením kabeláže elektrického napájania alebo dátových liniek, ktoré majú vplyv na prevádzku kritických základných služieb,
25. Zhotoviteľ je povinný zabezpečiť, aby bola počas celej doby prevádzky systému dostupná kapacita podporných aktív v rozsahu potrebnom na zaistenie funkčnosti, výkonnosti a bezpečnosti poskytovanej služby,
26. zmeny procesov a systémov podliehajú schválenému procesu riadenia zmien aj z pohľadu riadenia bezpečnosti.
27. Každá zmena s potenciálnym dopadom na bezpečnosť alebo bezpečnostné opatrenia musí byť vopred posúdená a schválená Manažérom informačnej a kybernetickej bezpečnosti PZS.
28. Manažér informačnej a kybernetickej bezpečnosti PZS musí byť zapojený do procesu riadenia zmien od jeho inicializačnej fázy až po schválenie realizácie zmeny.
29. Servis a údržbu komponentov systému CRS je možné vykonávať:
    1. miestne z PTO, prostredníctvom Servis serveru v DMZ tunela,
    2. vzdialene z SSÚD, prostredníctvom Servis serveru v DMZ SSÚD,
    3. vzdialene, zabezpečeným pripojením cez „NGFW1 OT“ do Servis serveru (funkcia „Jump server“)
30. Pripájanie sa lokálne priamo na komponenty CRS alebo prostredníctvom nezabezpečených prvkov IKT je zakázané.
31. **Bezpečnostné opatrenia pre ochranu proti škodlivému kódu a nežiaducemu obsahu:**
32. Zhotoviteľ je povinný zabezpečiť, aby signatúry antivírusového a antimalvérového softvéru boli vždy aktuálne,
33. Zhotoviteľ je povinný zabezpečiť, aby prístup k externým internetovým zdrojom bol riadený a kontrolovaný s cieľom minimalizovať vystavenie systémov a používateľov škodlivému alebo neautorizovanému obsahu.
34. Riadenie prístupu sa zabezpečí najmä prostredníctvom:
    1. filtrovania a kontroly sieťovej prevádzky na úrovni firewallu alebo proxy,
    2. obmedzenia prístupu na schválené internetové zdroje,
    3. monitorovania komunikácie za účelom detekcie škodlivého obsahu.
35. **Bezpečnostné opatrenia pre systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť :**
36. Zaviesť a dodržiavať segmentáciu sietí, pričom informačné systémy so službami priamo prístupnými z externých sietí sa musia nachádzať v samostatných sieťových segmentoch a v rovnakom segmente sú len informačné systémy s podobným účelom,
37. prepojenia medzi segmentami a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií,
38. je používané šifrovanie na zabezpečenie vybraných údajov pri prenose medzi a v rámci rôznych úrovní systémov OT. Identifikácia vybraných údajov prebieha pomocou klasifikácie informácií, ktorá bude Zhotoviteľovi poskytnutá PZS. Toto opatrenie je relevantné pre komponenty zaradené do vrstiev pre operačné technológie 3 a vyššie,
39. smerovanie a filtrácia sieťovej prevádzky do a z externých sietí musí ísť cez sieťový firewall,
40. je zavedená logická ako aj fyzická segmentácia medzi operačnými technológiami, sieťami a informačnými systémami,
41. musí byť zabezpečená segmentácia hlavnej siete riadiaceho systému od ostatných sietí operačných technológií. Toto opatrenie je relevantné pre komponenty zaradené do vrstiev pre operačné technológie 3 a vyššie.
42. sieťový firewall pre operačné technológie je nezávislý od ostatných mechanizmov na smerovanie a filtráciu sieťovej prevádzky,
43. v sieťach určených pre operačné technológie je blokované odosielanie a prijímanie správ medzi používateľmi,
44. v sieťach určených pre operačné technológie je blokované odosielanie a prijímanie správ medzi používateľmi.
45. **Bezpečnostné opatrenia pre monitorovanie, zaznamenávanie a hlásenie udalostí .**

1. Zhotoviteľ je povinný zabezpečiť implementáciu a prevádzku nástrojov a opatrení na monitorovanie bezpečnosti siete informačných systémov v správe Zhotoviteľa, a to v rozsahu pokrývajúcom najmä:

1. monitorovanie prieniku škodlivého kódu do prostredia sietí IS,
2. identifikáciu neoprávnených sieťových spojení na rozhraní s vonkajšou sieťou,
3. udržiavanie aktuálnej evidencie vstupno-výstupných bodov na rozhraní sietí,
4. poskytovanie pravidelných reportov o zistených udalostiach, škodlivých kódoch, neoprávnených spojeniach a navrhovaných nápravných opatreniach.
5. Monitorovanie a evidencia podľa odseku 1 sa musia vykonávať automatizovaným nástrojom určeným pre prostredie OT/IS sietí, ktorý umožňuje:
   1. pasívnu analýzu sieťovej prevádzky,
   2. detekciu škodlivého kódu, anomálií a neautorizovaných spojení,
   3. generovanie reportov a export relevantných bezpečnostných udalostí do centrálneho systému pre správu bezpečnostných incidentov PZS (napr. SIEM/SOC). Na základe požiadavky PZS je Zhotoviteľ povinný v súčinnosti s PZS vykonať integráciu monitorovacieho systému do existujúceho SIEM/SOC riešenia PZS, vrátane nastavenia potrebných rozhraní, formátov prenosu údajov a overenia funkčnosti prenosu udalostí.
6. Zhotoviteľ je povinný zabezpečiť, aby všetky zistenia z monitorovania boli:
   1. evidované, vyhodnocované a archivované po dobu minimálne 12 mesiacov,
   2. v prípade incidentov bezodkladne eskalované podľa definovaného postupu reakcie na kybernetické incidenty,
   3. riešené v spolupráci s PZS a s príslušnými bezpečnostnými autoritami, ak to povaha incidentu vyžaduje.
7. Zhotoviteľ je povinný zabezpečiť, že žiadna zmena v konfigurácii sieťových rozhraní alebo bezpečnostných politík nebude vykonaná bez predchádzajúceho schválenia PZS.
8. Zhotoviteľ vytvorí technické podmienky pre nasadenie Security NDS boxu. Zhotoviteľ je povinný na základe požiadavky Objednávateľa pripraviť voľné sieťové porty a následne poskytnúť potrebnú súčinnosť na technické zabezpečenie a nastavenie zrkadlenia (mirroringu) sieťovej komunikácie na určený port, a to spôsobom, ktorý umožní jej ďalšiu analýzu alebo monitoring zo strany PZS alebo ním tretej strany.
9. V prípade, ak v čase dokončenia stavby a jej uvedenia do prevádzky nebude mať PZS zavedené a prevádzkované riešenie typu SIEM a/alebo SOC, je PZS povinný zabezpečiť vytvorenie a sprístupnenie prístupov do centrálnej konzoly (alebo iného primeraného rozhrania), prostredníctvom ktorej budú oprávneným osobám sprístupnené všetky relevantné bezpečnostné dáta generované používanými bezpečnostnými nástrojmi, a to minimálne v rozsahu potrebnom na monitorovanie, vyhodnocovanie bezpečnostných udalostí a incidentov. Takéto prístupy musia byť zriadené v rozsahu „read-only“, ak sa zmluvné strany nedohodnú inak, a musia byť dostupné po celú dobu prevádzky stavby.
10. **Bezpečnostné opatrenia pre fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení**
11. Zhotoviteľ je povinný dodržiavať pravidlá fyzickej bezpečnosti na pracoviskách PZS, vrátane povinnosti riadne evidovať vstupy, pohyb a odchody osôb Zhotoviteľa vo vyhradených priestoroch PZS v príslušných evidenčných knihách alebo systémoch určených na tento účel.
12. Zhotoviteľ fyzicky pristupuje a manipuluje len s tými aktíva, ktoré spadajú do predmetu hlavnej zmluvy,
13. je zakázané používanie prenosných zariadení v kritických oblastiach operačných technológií, tzn. kritické podporní aktíva.
14. Zhotoviteľ zabezpečí automatické uplatňovanie konfigurovateľných obmedzení v prostredí OT, ktoré zabránia používaniu neautorizovaných prenosných a mobilných zariadení, budú vyžadovať primeranú autorizáciu prístupu a obmedzia prenos kódu a dát medzi týmito zariadeniami a OT systémami. Toto opatrenie je relevantné pre komponenty zaradené do vrstiev operačné technológie 3 a vyššie.
15. **Bezpečnostné opatrenia pre ochranu záznamov, súkromia a označovanie informácií**
16. Zhotoviteľ je povinný dodržiavať klasifikáciu informácií a záznamov stanovenú PZS a zabezpečiť ich ochranu a označovanie v súlade s touto klasifikáciou. Klasifikácia informácií zahŕňa najmä určenie úrovne citlivosti, spôsobu označovania, prístupu, uchovávania a prenosu, pričom Zhotoviteľ je povinný tieto požiadavky uplatňovať v plnom rozsahu aj u svojich subdodávateľov.
17. **Všeobecná požiadavka**
18. Všetky dokumenty zo strany Zhotoviteľa preukazujúce výkon požadovaných činností musia byť predložené v jednotnom formáte (PDF, XLSX, DOCX), pomenované podľa NDS vzoru KB\_<oblasť>\_<dátum>\_<verzia>. Každý súbor obsahuje informácie kto je : zodpovedná osoba, dátum, verzia, prípadne posledný schvaľovateľ. V prípade, že sa jedná o doklad vo formáte Log súboru, ten musí byť otvoriteľný a čitateľný v balíku SW MS OFFIC 365 alebo notes v OS Windows 10 plus vyššou verziou. Log súbor je na vyžiadanie Zhotoviteľ povinný zaslať bezodkladne, najneskôr však do 3 kalendárnych dní v zaheslovanej forme na emailovú adresu orb@ndsas.sk a mikb@ndsas.sk. Heslo k súboru poskytne schvaľovateľom inou dohodnutou komunikačnou formou (SMS, telefonicky). V prípade nejasností v procese schválenia vykonaných prác, má vedúci odboru riadenia bezpečnosti, prípadne ním určený zástupca a expert manažér informačnej a kybernetickej bezpečnosti právo si vyžiadať doplňujúce podklady podľa potreby.
19. Za doložiteľné preukazujúce formy k jednotlivým činnostiam definovaných v špecifikácií ceny za plnenie povinností vyplývajúcich zo Zmluvy KB Objednávateľ považuje:

I. Zaškolenie technického personálu v oblasti OT/IT bezpečnosti

a. Prezenčná listina s podpisom účastníkov

b. Program školenia / agenda

c. Prezentácie, študijné materiály

d. Výstupy zo záverečného testu preškolených zamestnancov so záznamom úspešnosti , tak aby nebolo porušené GDPR

II. Preventívne a nápravné opatrenia + preverenie opatrení

a. Protokoly o návrhoch opatrení

b. Schvaľovacie záznamy Objednávateľa

c. Fotodokumentácia / konfiguračné výpisy

d. Testovacie protokoly po realizácii

III. Analýza a vyhodnotenie informácií o závažných incidentoch

a. Incident reporty podľa Zákona o kybernetickej bezpečnosti

b. Chronológia postupu vyšetrovania

c. Forenzné výstupy, logy

d. Návrhy nápravných opatrení

IV. Zoznamy prístupových práv a privilégií

a. Exporty zo systémov (anonymizované, ak treba)

b. História zmien rolí a práv

c. Protokoly o revízii prístupov

V. Hodnotenie zraniteľností a hlásenie nálezov

a. Výstup zo skenovacích nástrojov

b. CVE/CVSS hodnotenia

c. Hlásenie zraniteľnosti pre Objednávateľa (kópie emailov, kópia korešpondencie)

d. Prehľad zraniteľností a návrhov na zlepšenie bezpečnostného rámca

VI. Evidencia záplat vykonaných Dodávateľom

a. Patch logy z nástrojov

b. Report o stave aktualizácií pred/po

c. Schválenia od Objednávateľa pri kritických zásahoch

VII. Konfigurácia a nastavenie mirroringu

a. Konfiguračné výpisy pred/po

b. Dokumentácia architektúry a topológií

c. Logy

VIII. Aktualizácia zoznamu funkčných členov / aktív

a. Aktualizovaný zoznamov aktív

IX. Mimoriadny patch manažment

a. Incident/change ticket

b. Logy z nástroja, výsledok inštalácie

X. Súčinnosť pri auditoch bezpečnosti

a. Protokoly o poskytnutí súčinnosti

b. Zápisy z auditných stretnutí

c. Evidované vstupy Dodávateľa

XI. Súčinnosť pri penetračných testoch CRS

a. Reporty z testov (aspoň časť relevantná Dodávateľovi)

b. Logy účasti pri riešení zistení

c. Tickety o nápravných opatreniach

XII. Súčinnosť pri BCM a plánoch obnovy

a. Aktualizovaná dokumentácia BCM

b. Podpisová stránka o prebraní aktualizácií

c. Emailové komunikácie súvisiace sú súčinnosťou Objednávateľovi

d. Účasť na workshopoch (prezenčná listina)

**Vysvetlenie pre opatrenia podmienené relevantnosťou pre komponenty zaradené do vrstiev pre operačné technológie 3 a vyššie:**

**Vrstvami pre operačné technológie je nasledovné rozdelenie prostredí, ktoré majú vplyv na prevádzkované operačné technológie:**

vrstva 5 – celkové prostredie organizácie

vrstva 4 – prostredie pre centrálnu správu operačných technológií,

vrstva 3 – prostredie pre prevádzku a riadenie výrobného procesu, najmä zálohovací server (historian), riadiace servery,

vrstva 2 – prostredie pre riadenie a automatizáciu procesov, najmä rozhranie človek-stroj (HMI), dispečerské riadenie a zber dát (SCADA),

vrstva 1 – prostredie priameho riadenia, najmä programovateľné logické automaty (PLC),

vrstva 0 – fyzické prostredie, najmä senzory, akčné členy.

1. Podporné aktíva = všetky technické, softvérové, komunikačné a personálne prostriedky, ktoré podporujú prevádzku hlavného systému alebo služby.

   Sem patria: servery, úložiská, záložné zdroje, siete, komunikačné linky, virtualizačné platformy, databázové servery, nástroje na monitorovanie a správu, a aj personálne alebo organizačné zdroje (napr. servisný personál, podpora subdodávateľov). [↑](#footnote-ref-1)
2. Vrstvami pre operačné technológie je nasledovné rozděleni prostredia, ktoré majú vplyv na prevádzkované operačné technológie:

   vrstva 5 – celkové prostredie organizácie

   vrstva 4 – prostredie pre centrálnu správu operačných technológií,

   vrstva 3 – prostredie pre prevádzku a riadenie výrobného procesu, najmä zálohovací server (historian), riadiace servery,

   vrstva 2 – prostredie pre riadenie a automatizáciu procesov, najmä rozhranie človek-stroj (HMI), dispečerské riadenie a zber dát (SCADA),

   vrstva 1 – prostredie priameho riadenia, najmä programovateľné logické automaty (PLC),

   vrstva 0 – fyzické prostredie, najmä senzory, akčné členy. [↑](#footnote-ref-2)