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

# (ďalej len „Zmluva KB“)

medzi zmluvnými stranami:

Názov: Národná diaľničná spoločnosť, a. s.

Sídlo: Dúbravská cesta 14, 841 04 Bratislava, Slovenská republika

IČO: 35 919 001

DIČ: 202 193 7775

IČ DPH: SK2021937775

V mene ktorého koná: Ing. Filip Macháček, predseda predstavenstva a generálny riaditeľ

XYZ,Člen predstavenstva

Registrácia: Akciová spoločnosť zapísaná v Obchodnom registri Mestského

súdu Bratislava III, oddiel Sa, vložka č. 3518/B

Bankové spojenie (názov banky):

IBAN:

SWIFT kód:

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

a

Názov: ...........................

Sídlo: ...........................

IČO: ............................

IČ DPH: ............................

Zastúpený: ............................

Zapísaný: ............................   
(ďalej len „**Zhotoviteľ**“)

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

**Článok I.**

ÚVODNÉ USTANOVENIA

1. **Národná diaľničná spoločnosť, a. s.** je podľa § 18 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 Informačný systém diaľnic a rýchlostných ciest.** Zhotoviteľ ako dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako Prevádzkovateľa kritickej základnej služby.
2. Zhotoviteľ uzatvoril s Prevádzkovateľom základnej služby **Zmluvu o dielo – XXX zo dňa xx.xx.xxxx** (ďalej len „**hlavná zmluva**“), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v ZoKB pre Prevádzkovateľa kritickej základnej služby (ďalej aj ako „**hlavný zmluvný vzťah**“). Konkrétny rozsah činností Zhotoviteľa je identifikovaný v hlavnej zmluve.
3. 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.
4. V súlade s ustanovením § 19 ods. 2 ZoKB je Prevádzkovateľ kritickej základnej služby povinný pri uzatvorení zmluvy s Zhotoviteľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa kritickej základnej služby uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti hlavnej zmluvy.

**Článok II.**

ZÁKLADNÉ POJMY

1. Na účely tejto Zmluvy KB sa rozumie:
2. sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,
3. kybernetickým priestorom globálny, dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,
4. kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti   
   a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
5. dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
6. dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
7. integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
8. kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,
9. rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
10. hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam   
    a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
11. kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia definovaných bezpečnostných opatrení z bezpečnostnej politiky ( v Prílohe č. 2 tejto Zmluvy)alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
12. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
13. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
14. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
15. ohrozenie bezpečnosti informácií,
16. udalosťou odvrátenou v poslednej chvíli udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo,
17. zraniteľnosťou akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou,
18. kritickou základnou službou služba, ktorá je spĺňa náležitosti § 18 ZoKB.
19. prevádzkovateľom základnej služby ten, kto je zapísaný v registri prevádzkovateľov základnej služby.
20. digitálnou službou služba, ktorej druh je uvedený prílohe č. 2 ZoKB,
21. manažér informačnej a kybernetickej bezpečnosti (ďalej len „**MIKB**“) je osoba poverená riadením informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti definované v Politike informačnej a kybernetickej bezpečnosti a ďalších smerniciach Prevádzkovateľa kritickej základnej služby. Ide najmä o kontrolné činnosti, riešenie kybernetických bezpečnostných incidentov, riadenie implementácie bezpečnostných opatrení, konzultačné a metodické činnosti pre oblasť informačnej a kybernetickej bezpečnosti a ďalšie,
22. riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace   
    s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov,
23. významnou kybernetickou hrozbou kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál spôsobiť závažný kybernetický bezpečnostný incident alebo môže mať iný závažný vplyv na sieť a informačný systém subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú škodu,

**Článok III.**

**PREDMET ZMLUVY**

1. V zmysle § 19 ods. 2 ZoKB a s ohľadom na hlavnú zmluvu, je predmetom tejto Zmluvy KB úprava práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti hlavnej zmluvy.
2. Prevádzkovateľ kritickej základnej služby je povinný v zmysle § 19 ods. 2 ZoKB uzatvoriť s Zhotoviteľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Obsah zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností definuje a ustanovuje § 9 ods. 2 Vyhlášky č. 362/2018 Z.z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej aj „**Vyhláška NBÚ**“).
3. V rámci tejto Zmluvy KB je potrebné stanoviť základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa kritickej základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Prevádzkovateľa kritickej základnej služby a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany Prevádzkovateľa kritickej základnej služby (ďalej len „**ciele**“), a to aj v spolupráci s Zhotoviteľom.
4. Prevádzkovateľ kritickej základnej služby a Zhotoviteľ pri riešení incidentov podľa článku VI., bod 1 tejto Zmluvy KB a implementácií reaktívnych opatrení podľa článku VI., bod 2 tejto Zmluvy KB a ochranných opatrení podľa článku VI., bod 6 tejto Zmluvy KB budú postupovať podľa usmernení vládnej jednotky pre riešenie počítačových incidentov, so zreteľom na oznámenia a varovania špecifikované na web stránkach www.csirt.gov.sk, www.nbu.gov.sk, www.sk-cert.sk.

**Článok IV.**

**PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN**

1. Zhotoviteľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa kritickej základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve KB tak, aby boli naplnené ciele tejto Zmluvy KB. Zoznam bezpečnostných opatrení Prevádzkovateľa kritickej základnej služby a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v prílohe č. 2 tejto Zmluvy KB.
2. Zhotoviteľ sa zaväzuje riadiť sa stanovenými bezpečnostnými opatreniami v tejto Zmluve KB.
3. Zhotoviteľ je povinný dodržiavať definované bezpečnostné opatrenia vyplývajúce z bezpečnostných politík Prevádzkovateľa kritickej základnej služby, ktoré sú definované v Prílohe č. 2 tejto Zmluvy KB, a ktoré sa týkajú poskytovania služby podľa hlavnej zmluvy.. Zhotoviteľ sa s nimi preukázateľne oboznámil, a to v rozsahu v akom súvisia s prevádzkovaním základnej služby Prevádzkovateľom základnej služby, a zároveň v akom ich je možné aplikovať na služby uvedené v článku I. bod 2 Zmluvy a potvrdzuje to podpisom tejto Zmluvy.
4. Zhotoviteľ  berie na vedomie, že požadované opatrenia z bezpečnostných politík Prevádzkovateľa kritickej 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 kritickej základnej služby. Prevádzkovateľ kritickej základnej služby sa zaväzuje o takýchto plánovaných zmenách Zhotoviteľa informovať najneskôr 30 (tridsať) dní pred ich implementovaním.
5. Zhotoviteľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve KB tak, aby boli naplnené ciele tejto Zmluvy KB. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto Zmluvy KB.
6. Zhotoviteľ, prípadne jeho subdodávateľ zabezpečujúci príslušné činnosti, vyhlasuje, že disponuje so všetkým potrebným technickým, technologickým a personálnym vybavením, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy KB, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto Zmluvy KB pre identifikáciu prípadne pre opravu poruchy/incidentu a zabezpečenie bezpečnej prevádzky IS.
7. Odplata za plnenie povinností Zhotoviteľa podľa tejto Zmluvy KB a náhrada všetkých nákladov vynaložených Zhotoviteľom v súvislosti s plnením povinností Zhotoviteľa podľa tejto Zmluvy KB sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom základnej služby Poskytovateľovi/Zhotoviteľovi podľa hlavnej zmluvy a na žiadne ďalšie peňažné plnenia Zhotoviteľ za plnenie povinností podľa tejto Zmluvy KB od Prevádzkovateľa kritickej základnej služby nemá nárok.
8. 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 kritickej základnej služby namiesto Zhotoviteľa alebo spolu s Zhotoviteľom. Zhotoviteľ sa zaväzuje, že nezapojí ďalšieho subdodávateľa predtým, než dostane písomný súhlas Prevádzkovateľa kritickej základnej služby.
9. Zoznam subdodávateľov tvorí prílohu č. 3 tejto Zmluvy KB. Zhotoviteľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Zhotoviteľa uvedené v tejto Zmluve KB. Zhotoviteľ je plne zodpovedný voči Prevádzkovateľovi kritickej základnej služby za plnenie povinností subdodávateľa.
10. Pre vylúčenie akýchkoľvek pochybností sa Zhotoviteľ zaväzuje plniť podmienky tejto Zmluvy KB vrátane podmienok budúcej legislatívy Európskej Únie  transponovanej do legislatívy  Slovenskej republiky počas účinnosti tejto Zmluvy KB, hlavne no nie výlučne Smernice o bezpečnosti sietí a informácií NIS 2 (Smernica Európskeho parlamentu a rady (EÚ) 2022/2555 zo 14. decembra 2022), pokiaľ sa na neho budú vzťahovať. Prípadné úpravy a doplnenia činností KB budú zmluvné strany riešiť na základe analýzy rizík.
11. Zhotoviteľ sa zaväzuje, počas trvania hlavnej zmluvy, najneskôr do troch (3) dní od zmeny údajov, Prevádzkovateľovi kritickej základnej služby 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 NDS, a.s. 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, a budú využité výhradne v krízovej situácii po písomnom informovaní Zhotoviteľa Prevádzkovateľom základnej služby.
12. Zhotoviteľ sa zaväzuje, po skončení trvania hlavnej zmluvy, najneskôr do troch (3) dní Prevádzkovateľovi kritickej základnej služby 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 NDS, ako aj všetky ďalšie súvisiace prístupy pre zabezpečenie funkčného a bezproblémového prevzatia systémov a zachovania kontinuity činnosti.

**Článok V.**

**POŽADOVANÝ ROZSAH ČINNOSTÍ DODÁVATEĽA**

1. Zhotoviteľ je povinný v rámci zabezpečenia bezpečného fungovania kritickej základnej služby Prevádzkovateľa kritickej základnej služby a predchádzaniu kybernetickým bezpečnostným incidentom, ktoré by mohli mať potenciálne nepriaznivý vplyv na základnú službu Prevádzkovateľa kritickej základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa kritickej základnej služby v súvislosti s poskytovaním služby podľa hlavnej zmluvy (ďalej len „**incidenty**“ v príslušnom gramatickom tvare):
2. zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Zhotoviteľa a jeho subdodávateľov nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa kritickej základnej služby,
3. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy KB alebo budú mať prístup k informáciám Prevádzkovateľa kritickej základnej služby,
4. sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
5. sledovať hrozby, dotýkajúce sa Zhotoviteľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na kritickú základnú službu Prevádzkovateľa kritickej základnej služby,
6. predchádzať vzniku incidentov,
7. poskytnúť súčinnosť Prevádzkovateľovi kritickej základnej služby pri systematickom získavaní (monitorovaní a detegovania), sústreďovaní (evidovaní), analyzovaní a vyhodnocovaní informácií o incidentoch ( t.j. súčinnosť = vytvorenie technických podmienok k inštalácií NDS Box v zmysle Tešp04),
8. prijímať od Prevádzkovateľa kritickej základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa kritickej základnej služby,
9. spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa kritickej základnej služby.
10. Zhotoviteľ je povinný stanoviť postupy plnenia svojich povinností podľa Zmluvy KB vo vlastnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; a túto dokumentáciu je na odôvodnené požiadanie ( napr. výkon auditu, prípadne kontrola plnenia opatrení) povinný predložiť Prevádzkovateľovi kritickej základnej služby na nahliadnutie. Nejedná sa v tomto prípade o bezpečnostnú dokumentáciu v zmysle ZoKB ale procesnú dokumentáciu Zhotoviteľa.
11. Zhotoviteľ je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 v aktuálne platnej verzii (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom v v bezpečnostných politikách Prevádzkovateľa kritickej základnej služby, ktoré sú definované v prílohe č. 2 tejto Zmluvy KB.
12. Zhotoviteľ je povinný prijať a dodržiavať bezpečnostné opatrenia najmenej v oblastiach podľa § 20 ods. 2 písm. d), g), h), i), k) a m) (ZoKB po 1.1.2025 - b), d), , j), l), m) a n)) ZoKB v rozsahu podľa § 8, § 11 až § 13, § 15 a § 17 Vyhlášky NBÚ, špecifikovaných v bezpečnostných opatreniach, ktoré sú prílohou č. 2 tejto Zmluvy.
13. Zhotoviteľ je povinný prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom  v Prílohe č. 2 tejto Zmluvy KB.
14. Zhotoviteľ je povinný písomne informovať Prevádzkovateľa kritickej základnej služby o každej jemu preukázateľne známej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Zhotoviteľ alebo o všetkých jemu preukázateľne známych skutočnostiach, majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti; tým nie sú dotknuté povinnosti a zodpovednosť Prevádzkovateľa kritickej základnej služby v zmysle ZoKB, osobitných predpisov a/alebo ich vykonávacích predpisov.
15. 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 Prevádzkovateľa kritickej základnej služby, je uvedený v prílohe č. 1 tejto Zmluvy KB. Zhotoviteľ je povinný bezodkladne písomne oznámiť Prevádzkovateľovi kritickej základnej služby každú zmenu v personálnom obsadení; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB. Zhotoviteľ je povinný zaviazať povinnosťou mlčanlivosti podľa ZoKB osoby, ktoré sa budú podieľať na plnení podľa tohto bodu Zmluvy KB.

**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. Zhotoviteľ sa zaväzuje v čase detekcie kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi kritickej základnej služby.
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 kritickej 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 kritickej základnej služby povinný predložiť Prevádzkovateľovi kritickej 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 kritickej základnej služby preveriť jeho efektívnu účinnosť. Zmluvné strany sa dohodli, že účinnosť ochranných opatrení bude podmienená výkonom simulovaných útokov, pričom záver takýchto simulovaných útokov bude vyhodnotený na základe protokolu o efektívnom účinku ochranného opatrenia za Prevádzkovateľa kritickej základnej služby signovanom MIKB a za Zhotoviteľa signovanom osobou.

**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 kritickej základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa kritickej základnej služby. Zhotoviteľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Poskytovateľovi/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 kritickej 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.

**Článok VIII.**

**Povinnosti po skončení Zmluvy**

* 1. Po ukončení tejto Zmluvy KB je Zhotoviteľ povinný vrátiť alebo previesť na Prevádzkovateľa kritickej základnej služby všetky informácie, ku ktorým mal počas trvania tejto Zmluvy KB prístup, resp. podľa písomného pokynu Prevádzkovateľa kritickej základnej služby zabezpečí preukázateľné zničenie akýchkoľvek nosičov elektronickej informácie certifikovanou organizáciu, a doložením protokolu s podpismi oprávnených osôb Zhotoviteľa a objednávateľa.
  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 kritickej 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 kritickej 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. Zmluvná strana zodpovedá 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 vznikne Prevádzkovateľovi kritickej 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.
  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 10 (desať) 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, pričom Zhotoviteľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií (napr. PGP šifrovanie).
2. Prevádzkovateľ kritickej 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 kritickou základnou službou, pokiaľ to nie je v tejto Zmluve KB alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
6. V prípade, ak Zhotoviteľ plní Zmluvu KB prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa kritickej základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa kritickej 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 kritickej 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 kritickej základnej služby je podmienené aj odoslaním SMS MIKB podľa ustanovenia článku VI bod 2 Zmluvy KB.
8. Prevádzkovateľ kritickej základnej služby je oprávnený, na základe identifikácie skutočností vyplývajúcich z analýzy rizík, určiť, že Zhotoviteľ má významný vplyv na zabezpečenie kybernetickej bezpečnosti kritickej základnej služby.
9. V prípade, že analýza rizík Prevádzkovateľa kritickej základnej služby potvrdí významný vplyv Zhotoviteľa na zabezpečenie kybernetickej bezpečnosti kritickej základnej služby, Prevádzkovateľa kritickej základnej služby je povinný túto skutočnosť nahlásiť Národnému bezpečnostnému úradu (ďalej len „NBÚ“).
10. NBÚ následne podnet posúdi a v súlade s § 17 ods. 1 písm. i) a ods. 3 ZoKB Zhotoviteľa do registra prevádzkovateľov základnej služby.
11. Zhotoviteľ je povinný poskytnúť Prevádzkovateľovi všetku potrebnú súčinnosť pri plnení povinností vyplývajúcich z tohto článku.

# 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.

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 XIII**

**AUDIT KYBERNETICKEJ BEZPEČNOSTI /BEZPEČNOSTNÝ AUDIT**

1. Prevádzkovateľ kritickej základnej služby je oprávnený vykonať na dotknutom diele, v rámci ktorého sa nachádza kritická základná služba Prevádzkovateľ kritickej základnej služby pod voči Zhotoviteľovi ako aj u jeho subdodávateľov audit zameraný na overenie plnenia povinností Zhotoviteľa a subdodávateľov podľa tejto Zmluvy KB 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 a technológií v organizačnej, personálnej a technickej oblasti u Zhotoviteľa a subdodávateľov pre plnenie cieľov tejto Zmluvy KB.
2. Prevádzkovateľ kritickej základnej služby Prevádzkovateľ kritickej základnej služby. 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.
3. Prevádzkovateľ kritickej základnej služby môže audit voči Zhotoviteľovi a subdodávateľom realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa kritickej základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
4. 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.
5. Prevádzkovateľ kritickej 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.
6. V rámci auditu sú Zhotoviteľ a subdodávatelia povinní preukázať Prevádzkovateľovi kritickej 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.
7. Prevádzkovateľ kritickej základnej služby sa zaväzuje oznámiť Poskytovateľovi/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.
8. Zhotoviteľ sa zaväzuje písomne informovať Prevádzkovateľa kritickej základnej služby v zmysle komunikačnej matice o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Zhotoviteľom.
9. Prevádzkovateľ kritickej základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku VII. ods. 2, 3 a 4 tejto Zmluvy KB sa uplatňujú primerane.
10. Prevádzkovateľ kritickej 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 kritickej 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 kritickej 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.
11. Pre vylúčenie akýchkoľvek pochybností sa Zhotoviteľ zaväzuje zabezpečiť Prevádzkovateľovi kritickej základnej služby vykonanie auditu v zmysle tohto článku tejto Zmluvy KB aj u svojich subdodávateľov.
12. Zhotoviteľ v súlade s ods. 6.1.4.4 Technických Podmienok č.29/2008 - Zariadenia, infraštruktúra a systémy technologického vybavenia (ďalej len „TP 29") je povinný vykonať minimálne raz ročne bezpečnostný audit. Všetky systémy sa pred uvedením do prevádzky musia podrobiť bezpečnostnému auditu podľa ods. 13.1.6. TP 29.
13. Bezpečnostný audit sa musí počas prevádzky systému pravidelne opakovať, a to minimálne 1x ročne, počas jarnej odstávky.
14. Výstup bezpečnostného auditu v zmysle TP 29 bude Prevádzkovateľom kritickej základnej služby použitý na účely zisťovania nedostatkov týkajúcich sa informačnej bezpečnosti a prípravy podkladu pre Audit kybernetickej bezpečnosti.

**Článok XIV.**

**SANKCIE**

1. Zmluvné strany sa dohodli, že v prípade porušenia ktorejkoľvek povinnosti Poskytovateľa uvedenej v bode 1 až 7 prílohy č. 2 tejto Zmluvy je Objednávateľ 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 kritickej 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 kritickej základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Zhotoviteľom.

1. Zmluvné strany sa dohodli, že uplatnením sankcií v zmysle tohto článku Zmluvy KB nie je dotknutý nárok Prevádzkovateľa kritickej základnej služby na náhradu škody, ktorá mu vznikla porušením povinností Zhotoviteľa.
2. 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 kritickej 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.
8. Po zániku tejto Zmluvy KB je Zhotoviteľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa kritickej základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom základnej služby. Licenčné podmienky sa riadia časťou 17. 5. A hlavnej zmluvy, t.j. Zmluva o dielo.

**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 kritickej 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, GDPR)**
* Príloha č. 2 - Špecifikácia a rozsah bezpečnostných opatrení -

(vyplývajúce z Bezpečnostných smerníc Prevádzkovateľa kritickej základnej služby),**(nezverejňuje sa v CRZ)**

* Príloha č. 3 – Vzor - Záznam o kybernetickom bezpečnostnom incidente
  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 kritickej základnej služby**: |  | **Zhotoviteľ:** |

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(obchodné meno) (obchodné meno)

(titul, meno, priezvisko (titul, meno, priezvisko

štatutára) štatutára)

(funkcia) (funkcia)

**Príloha č. 1:** Zoznam pracovných rolí a kontaktov Prevádzkovateľa kritickej základnej služby a Zhotoviteľa (**nezverejňuje sa v CRZ,GDPR)**

Prevádzkovateľ kritickej základnej služby:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Meno a priezvisko** | **Rola** | **Proces súvisiaci s prevádzkou ZS** | **Telefónny kontakt** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Zhotoviteľ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Meno a priezvisko** | **Rola** | **Proces súvisiaci s prevádzkou ZS** | **Telefónny kontakt** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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

Plnením bezpečnostných opatreniami a všetkých činností v zmysle zákona č.69/2018 Z. z. o kybernetickej bezpečnosti sa rozumejú činnosti nad prostredím dotknutej prevádzkovanej základnej služby, a nejedná sa o interné prostredie Zhotoviteľa. Požadované plnenie politík a postupov, sa taktiež týka výhradne dotknutej prevádzkovanej základnej služby.

1. **Pre oblasť riadenia prístupov realizuje Zhotoviteľ opatrenia podľa § 8 Vyhlášky NBÚ č. 362/2018, Z.z., prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:**
   1. dodržiavanie zásad riadenia prístupu k informáciám,
   2. riadenia prístupu používateľov v rámci dotknutých systémov pod hlavnou zmluvou;
   3. dodržiavanie a vymedzenie príslušných zodpovedností používateľov a rolí;
   4. riadenia prístupu k sieťam, čím sa rozumie:
      1. že každému používateľovi siete a informačného systému sa prideľuje jednoznačný identifikátor na autorizovaný vstup do siete a informačného systému;
      2. zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane ich prístupových práv;
      3. využívanie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroja na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy);
      4. na vyzvanie poskytnúť súčinnosť pre Objednávateľa pri výkone kontroly súladu schválených používateľských účtov a prístupových oprávnení v pravidelných intervaloch, najmenej však raz ročne, a to vo forme poskytnutia aktuálneho výpisu pridelených prístupových oprávnení do IS a podporných systémov a v prípade ich nesúladu následné bezodkladné deaktivovanie, resp. zmazanie;
      5. určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle bezpečnostnej stratégie alebo príslušnej bezpečnostnej politiky Objednávateľa. (Určenú zodpovednú osobu požaduje Objednávateľ aj na strane Zhotoviteľa ako aj na strane Objednávateľa).
   5. riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa.
   6. Objednávateľ požaduje:
      1. Prideľovať a odoberať prístupy iba na základe požiadavky gestora prevádzkovanej základnej služby, alebo ním určenej oprávnenej osoby,
      2. V prípade potreby poskytnutie súčinnosti pri aktualizácií Evidencie prístupov, ktorú vedie Zhotoviteľ,
      3. 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 ich pracovné úlohy,
      4. Zabezpečiť logovanie aktivít, a to všetkých prístupov a aktivít používateľov v systéme,
      5. Zabezpečiť monitorovanie v reálnom čase, a to použitím nástroja na sledovanie a analýzu prístupových záznamov v reálnom čase.
   7. riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb Prevádzkovateľa kritickej základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
   8. musí byť využívaná funkcia zabezpečeného prístupu do systému formou protokolu mechanizmu AAA (Authentication-Authorization-Accounting),
   9. kópia hesiel k privilegovaným účtov ( k účtom s najvyššími oprávneniami systémov) musí byť v čase prevádzky uložená v zabezpečenej schválenej forme u Objednávateľa v zabezpečenom priestore.
2. **Pre oblasť technických zraniteľností systémov a zariadení realizuje Zhotoviteľ opatrenia podľa § 11 Vyhlášky NBÚ č. 362/2018 Z.z., identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Objednávateľovi a ktoré toto poskytovanie služieb Objednávateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledujúcich bodoch alebo opatrení s porovnateľným účinkom:**
   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 ročne pre všetky sieťové aktíva a minimálne raz štvrťročne pre aktíva určené ako kritické. 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 vyšším CVSS 3.0 ako hodnota 7.0, Zhotoviteľ poskytne Objednávateľovi zoznam týchto identifikovaných zraniteľností aj s určeným dotknutých aktív.
   6. Zhotoviteľ zabezpečí identifikáciu potrieb softvérových záplat a aktualizácií, ako aj zabezpečuje ich implementáciu.
   7. Zhotoviteľ vedie evidenciu softvérových záplat a aktualizácií a informácie o ich nasadení alebo o dôvodoch nenasadenia, a na požiadanie je povinný ju poskytnúť Objednávateľovi. V prípade rozhodnutia Zhotoviteľa nenasadiť bezpečnostnú záplatu alebo aktualizáciu je povinný Zhotoviteľ informovať MIKB Objednávateľa o dôvodoch nenasadania.
   8. Zhotoviteľ je povinný testovať softvérové záplaty a aktualizácie pred ich nasadením do ostrej prevádzky systému,
   9. Zhotoviteľ je povinný aktualizovať plány softvérových záplat a aktualizácií.
3. **Pre oblasť ochrany proti škodlivému kódu, realizuje Zhotoviteľ opatrenia podľa §12 Vyhlášky NBÚ č. 362/2018, Z.z., prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:**
4. Inštalovať a aktualizovať antivírusový softvér na všetkých zariadeniach, ak to daná technológia umožňuje,
5. Všetky oprávnené osoby s prístupov do systému ( t. j. používateľov technológie) musia byť preškolení v rámci prevencie pred škodlivým kódom,
6. Všetci používatelia sú povinní dodržiavať pravidlá alebo postupy, aby sa zabránilo vniknutiu škodlivého softvéru (ako sú vírusy, malware, trojany a podobne) do počítačových systémov.
7. Je povolené vyberať len overené antivírusové a antimalware programy od renomovaných výrobcov.
8. Zhotoviteľ je povinný zabezpečiť, aby antivírusový a antimalware softvér (signatúry) bol vždy aktuálny.
9. Zhotoviteľ je povinný naplánovať a vykonávať pravidelné skenovanie systémov na detekciu škodlivého kódu minimálne raz štvrťročne.
10. Zhotoviteľ je povinný nastaviť systém na monitorovanie a automatické upozorňovanie na podozrivé aktivity.
11. Zhotoviteľ je povinný zabezpečiť monitorovanie potenciálnych ciest prieniku škodlivého kódu do prostredia sietí a informačných systémov prevádzkovanej základnej služby.
12. **Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje Zhotoviteľ opatrenia podľa §13 Vyhlášky NBÚ č. 362/2018, Z.z., prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:**
    1. riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov: servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
    2. prepojenia medzi segmentami a externými sieťami, musia byť chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií;
    3. bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup (napr. bezpečným spôsobom s použitím dvojfaktorovej autentifikácie alebo použitím kryptografických prostriedkov); Vzdialený prístup tretích strán ako Zhotoviteľa a jeho subdodávateľov v zmysle zmluvy do IS musí byť schválený Objednávateľom v zmysle vopred definovaných postupov.
    4. V prípade mimoriadnej situácie, napr. zásah pri bezpečnostnom incidente, pri prevádzkovom incidente môže byť vzdialený prístup schválený dodatočne najneskôr nasledujúci pracovný deň.
    5. opatrenia, že spojenia z  externých sietí sú smerované cez sieťový firewall a systém detekcie prienikov;
    6. serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu;
    7. udržiavania zoznamu všetkých vstupno-výstupných bodov na perimetri siete v aktuálnom stave;
    8. použitia automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou;
    9. blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje;
    10. zakázanie komunikácie a prevádzky aplikácií cez nevyužité porty;
    11. systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na perimetri siete;
    12. implementácie systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky formou IDS je povinné a v prípade technických možností bez vplyvu na funkciu informačných systémov sa požadujú aj IPS;
    13. použitia dvojfaktorovej autentizácie každého vzdialeného pripojenia do internej siete;
    14. vykonávania pravidelného 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,
    15. dodržiavať postupy a nastavenie systémov v zmysle schválenej technickej špecifikácie.
13. **Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Zhotoviteľ opatrenia podľa § 15 Vyhlášky NBÚ č. 362/2018, Z.z. v rozsahu potrebnom pre poskytovanie služieb pre Prevádzkovateľa.**

Prevádzkový monitoring sa uskutočňuje implementáciou nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho prevádzkový bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu:

* 1. sieťových prvkov a serverov, ktoré sú súčasťou predmetu zákazky,
  2. služieb prístupných do externých sietí, ak sú súčasťou predmetu zákazky.
  3. Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov musí vytvárať prevádzkové záznamy a zaznamenávať najmenej:
     1. aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených,
     2. iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,
     3. pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla,
     4. automatické varovné alebo chybové hlásenia systémov,
     5. detegované podozrivé alebo škodlivé aktivity a
  4. ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.

**Prevádzkové záznamy musia byť zabezpečené, a to najmenej tak, že**

* + 1. sú čitateľné výlučne osobám povereným ich analýzou,
    2. zamedzujú možnosti prepísania alebo vymazania záznamu,
    3. záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete,
    4. sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

1. **Pre oblasť riešenia KBI realizuje Zhotoviteľ opatrenia podľa § 17 Vyhlášky NBÚ č. 362/2018, Z.z., najmä deteguje a rieši KBI, ktoré môžu mať dopad na poskytovanie služieb Objednávateľovi. To zahŕňa napríklad prijatie opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:**
   1. oboznámenie sa s postupmi Objednávateľa pri riešení KBI a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú minimálne postupy hlásenia KBI voči Objednávateľovi.
   2. Zabezpečenie technických podmienok v zmysle ods. 5 tejto prílohy z dôvodu zabezpečenia plnenia povinností Objednávateľa s cieľom zabezpečiť monitorovanie a analyzovanie prevádzkových udalostí v sieťach a informačných systémoch, a to zabezpečiť:
      1. Súčinnosť pri detegovaníe KBI, prostredníctvom nástroja na detekciu KBI, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.
      2. Súčinnosť pri zbere a vyhodnocovanie relevantných informácií o KBI prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o KBI; vyhľadávanie a zoskupovanie záznamov súvisiacich s KBI; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako KBI; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných KBI, tzn. vytvorenie technických podmienok v zmysle Tešp 04 pre nasadenie NDS boxu,
   3. Súčinnosť pri riešení zistených KBI a zníženie následkov zistených KBI podľa pokynov Objednávateľa.
   4. Súčinnosť pri vyhodnocovaní spôsobov riešenia KBI po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI v súčinnosti s Objednávateľom,
   5. Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v prílohe č. 1 tejto Zmluvy a postupom a cez kontakty uvedené v prílohe č. 4 „Poriadku o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a. s. Objednávateľa“,
   6. Samotný spôsob a forma hlásenia bezpečnostné incidentu sa bude riadiť platným predpisom Objednávateľa – „Poriadok o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“.
2. **Bezpečnostné opatrenia- všeobecné**
   1. Zhotoviteľ je povinný poskytnúť súčinnosť Objednávateľa pri zabezpečovaní opatrení pre oblasť riadenia rizík a aktív, a to:
      1. Odovzdanie evidencie aktív a komponentov vo formáte určenom Objednávateľom,
      2. Poskytnutie súčinnosti pri technickom vykonávaní kompletnej inventarizácie všetkých aktív v čase prevádzky systému Zhotoviteľom pre Objednávateľa minimálne raz ročne,
      3. Zabezpečiť pravidelnú údržbu a aktualizácie technických zariadení a softvérov v zmysle hlavného zmluvného vzťahu,
      4. Zhotoviteľ musí prispôsobiť opatrenia na základe spätnej väzby od Objednávateľa a výsledkov hodnotení rizík v súlade s postupmi pre zmenové požiadavky definovanými hlavnou zmluvou,
      5. Objednávateľ s Zhotoviteľom musí pravidelne revidovať a aktualizovať opatrenia na riadenie rizík a ochranu aktív v súlade so zmenami v prostredí a novými hrozbami.

**Príloha č. 3:**

Záznam o kybernetickom bezpečnostnom incidente

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Záznam o kybernetickom bezpečnostnom incidente | | | | | | | | | | | |
| Názov bezpečnostného incidentu: |  | | | | | | Číslo bezpečnostného incidentu: | | | | **(Vyplní NDS)** |
| Dátum a čas vzniku bezpečnostného incidentu: |  | | Dátum a čas  hlásenia bezpečnostného incidentu: | | | | |  | | | |
| Bezpečnostný incident nahlásil: |  | | | | | | Funkcia a osobné číslo: | |  | | |
| Útvar/úsek/  spoločnosť: |  | Telefonický kontakt: |  | | | | Email: | |  | | |
| Bezpečnostný incident zaevidoval: |  | | | | | | Funkcia a osobné číslo: | |  | | |
| Dotknutá základná služba(príp. objekt) : |  | | | | | | | | | | |
| Dotknuté IS a riadiace systémy: |  | | | | | | | | | | |
| Popis incidentu: |  | | | | | | | | | | |
| Dotknutý útvar: |  | | | Odhadovaný dopad:  **(Vyplní NDS)** | | | Vyberte položku. | | | | |
| Kategória bezpečnostného incidentu:  **(Vyplní NDS)** | Vyberte položku. | Vstup/Spôsob hlásenia: | |
| Hlásenie incidentu do JISKB NBÚ SR  **(Vyplní NDS)** | Číslo:  Forma hlásenia (rozhranie JISKB, email):  Popis dotknutej základnej služby: | | | | | | | | | | |
| Popis a vyčíslenie možného dopadu:  **(Vyplní NDS)** |  | | | | | | | | | | |
| Popis vyšetrovania incidentu:  **(Vyplní dodávateľ aj NDS)** |  | | | | | | | | | | |
| Druh bezpečnostného incidentu: | Vyberte položku.  Iné (uviesť): | | Typ bezpečnostného incidentu: | | | Vyberte položku.  Iné (uviesť): | | | | | |
| Popis prijatých/navrhovaných opatrení: **(Vyplní dodávateľ aj NDS)** | | | | | | | | | | | |
| Opatrenie: | Popis opatrenia: | | | | Útvar/osoba zodpovedná  za riešenie: | | | | | Termín splnenia: | |
|  |  | | | |  | | | | |  | |
|  |  | | | |  | | | | |  | |
|  |  | | | |  | | | | |  | |
|  |  | | | |  | | | | |  | |
|  |  | | | |  | | | | |  | |
|  |  | | | |  | | | | |  | |
|  |  | | | |  | | | | |  | |
| Poznámky: |  | | | | | | | | | | |
| Zoznam príloh: |  | | | | | | | | | | |
| Podpisy zodpovedných osôb: | Hlásenie o KBI podal:  Hlásenie o KBI prijal:  Navrhované opatrenia schválil: | | | | | | | | | | |