**Príloha č. 8** – ***Bezpečnostné opatrenia pri plnení predmetu SLA Zmluvy – „Zmluva na správu, údržbu a servis monitorovacieho systému GPS“***

* 1. Poskytovateľ sa zaväzuje zaistiť bezpečnosť a odolnosť Systému voči aktuálne známym typom útokov a pred odovzdaním akejkoľvek zmeny Informačného systému vykonať akceptačné testovanie na prítomnosť známych zraniteľnosti. V prípade zistenia zraniteľností sa Poskytovateľ zaväzuje tieto zraniteľnosti odstrániť, vykonať akceptačné opätovné testovanie a zdokumentovaný výsledok testovania odovzdať Objednávateľovi spolu s dodávaným riešením.
  2. Poskytovateľ sa zaväzuje dodržiavať nasledovné bezpečnostné opatrenia a zásady pre oblasť ochrany osobných údov a zabezpečenie informačnej bezpečnosti:
     1. Opatrenia na ochranu osobných údajov
        1. Poskytovateľ musí zabezpečiť na základe požiadaviek Objednávateľa minimalizáciu dát. Zhromažďovanie a spracovanie osobných údajov musí byť obmedzené na rozsah potrebný na poskytovanie služieb a predmetu zmluvy.
        2. Poskytovateľ sa zaväzuje spracovávať údaje iba na základe platného právneho základu a v súlade s GDPR a ďalšími platnými predpismi definovanými Objednávateľom.
        3. Kde je to technicky možné, osobné údaje by musia byť pseudonymizované alebo anonymizované, aby sa minimalizovalo riziko ich zneužitia.
        4. Osobné údaje môžu byť prístupné len autorizovaným zamestnancom, ktorí ich potrebujú k plneniu pracovných povinností. Prístup musí byť riadený pomocou systémov overenia, ako sú dvojfaktorová autentifikácia a periodická revízia prístupov.
        5. Poskytovateľ musí viesť záznamy o všetkých spracovaniach osobných údajov a umožniť kontrolu zo strany klienta alebo regulačných orgánov.
        6. Všetky prenosy osobných údajov musia byť šifrované, či už ide o prenos medzi internými systémami alebo so systémami tretích strán.
        7. Údaje musia byť uchovávané len po dobu, ktorá je nevyhnutná na plnenie účelu spracovania v zmysle predmetu zmluvy, a následne bezpečne odstránené.
     2. Opatrenia na zaistenie informačnej a kybernetickej bezpečnosti:
        1. Musí byť zabezpečená implementácia riadenia prístupu, vrátane autentifikácie a autorizácie na základe rolí. Všetky prístupy do systému TDM a EMU musia byť kontrolované a zaznamenané.
        2. každému používateľovi siete a informačného systému sa prideľuje jednoznačný identifikátor na autorizovaný vstup do siete a informačného systému;
        3. 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 TDM a EMU a podporných systémov a v prípade ich nesúladu následné bezodkladné deaktivovanie, resp. zmazanie;
        4. 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.
        5. všetky vstupy aplikácií tvoriacich Informačný systém sú kontrolované na valídnosť a sú sanitované;
        6. je zapnutá len nutne potrebná funkcionalita, porty a IP adresy a všetky ostatné sú vypnuté;
        7. v prípade, že je nevyhnutné vykonávať správu Informačného systému na diaľku, je to možné vykonávať výhradne prostredníctvom šifrovaných protokolov a každý vzdialený zásah je zdokumentovaný, schválený Objednávateľom a záznam o zásahu je odovzdaný Objednávateľovi najneskôr v posledný deň daného mesiaca;
        8. Dáta musia byť šifrované na úrovni ukladania aj prenosu, s použitím šifrovacích štandardov, ako je AES-256 pre ukladanie a TLS pre prenos.
        9. všetky pôvodné a administrátorské účty sú zdokumentované a majú unikátne prvotné heslo zložené z náhodnej postupnosti aspoň 14 znakov;
        10. všetky administrátorské heslá a prístupové údaje a dokumentácia sú k dispozícií aj Objednávateľovi (minimálne v zalepenej obálke);
        11. privilegované prístupové práva do systémov súvisiacich s predmetom Zmluvy sa pridelia len na dobu nevyhnutnú na realizáciu požadovaného zásahu, maximálne však na šesť mesiacov za čo zodpovedá správca dotknutého informačného systému. Po tejto dobe musí byť prístupový účet deaktivovaný alebo opätovne reaktivovaný.
        12. Systém disponuje funkcionalitou pre zmenu používateľských a administrátorských mien a hesiel a funkcionalitou vypnutia používateľského účtu;
        13. Poskytovateľ musí detegovať narušenia, zabezpečiť zber logov a vykonávať pravidelný audit prevádzkovej bezpečnosti, ktorý odhalí akékoľvek anomálie alebo pokusy o neoprávnený prístup, príp. hrozby voči dotknutým systémom.
        14. Všetky komponenty dotknutých Informačných systémov TDM a EMU musia byť aktuálne a podporované výrobcom. Poskytovateľ je povinný zabezpečiť pravidelné aktualizácie systémov a softvéru, vrátane záplat a updatov a vedenie ich zoznamov. Postup pre aktualizácie a aplikáciu záplat musí byť zdokumentovaný a dodržiavaný. Na vyžiadanie je povinný Poskytovateľ predložiť evidenciu záplat a updatov Objednávateľovi.
        15. Poskytovateľ je povinný nasadiť antivírusový a antimalwarový softvér, ktorý bude pravidelne aktualizovaný a bude vykonávať automatické kontroly dotknutých systémov.
        16. Poskytovateľ je povinný zabezpečiť ochrana na dotknutej technológii proti DDoS a iným útokom. Je povinný využiť technológiu na ochranu proti distribuovaným útokom, ktoré zabezpečia dostupnosť systémov aj pri veľkom zaťažení.
        17. Poskytovateľ je povinný vykonať skeny zraniteľností alebo penetračné testy každého dodávaného riešenia pred jeho finálnym odovzdaním a Poskytovateľ sa zaväzuje nedostatky zistené týmto testovaním pred odovzdaním riešenia odstrániť;
        18. Všetky zmeny v Informačnom systéme musia byť zdokumentované a schválené a dokumentácia a zdrojové kódy sú poskytnuté Objednávateľovi bezpečným spôsobom najneskôr v čase nasadenia zmeny do produkčného prostredia, zároveň sa Objednávateľ zaväzuje  použiť zdrojové kódy, výlučne v prípade, keď nie je za účelom odstránenia Incidentu možné zabezpečiť prítomnosť Poskytovateľa a na základe preukázateľných inštrukcií Poskytovateľa; Poskytovateľ nenesie zodpovednosť za prípadné vady Informačného systému spôsobené zásahom Objednávateľa alebo akejkoľvek tretej strany, ktoré neboli zo strany Poskytovateľa odsúhlasené;
        19. Poskytovateľ je povinný zabezpečiť pravidelné zálohovanie kritických dát s ukladaním záloh na geograficky oddelené miesta, aby sa predišlo strate dát pri kybernetickom útoku alebo poruche.
        20. Poskytovateľ je povinný viesť evidenciu aktív a komponentov vo formáte určenom Objednávateľom a jej aktualizácia evidencie aspoň raz do roka a poskytnutie aktuálnej evidencie na vyzvanie Objednávateľom,
        21. Poskytovateľ musí prispôsobiť opatrenia na základe spätnej väzby od Objednávateľa a výsledkov hodnotení rizík v súlade s postupmi pre zmenové požiadavky definovanými hlavnou zmluvou,
        22. Poskytovateľ je povinný poskytnúť súčinnosť Objednávateľovi pri revidovaní a aktualizovaní opatrení na riadenie rizík a ochranu aktív v súlade so zmenami v prostredí a novými hrozbami minimálne raz ročne,
        23. Poskytovateľ je povinný navrhnúť a predložiť Objednávateľovi plány obnovy pre prípad havárie, ktorý umožní rýchle obnovenie systémov v prípade výpadku.
        24. Na vyžiadanie Objednávateľa je Poskytovateľ povinný sprístupniť dokumentáciu aktivít zamestnancov Poskytovateľa a tretích strán najneskôr do 24 hodín od požiadavky;
        25. Na vyžiadanie Objednávateľa je Poskytovateľ povinný poskytnúť plnú súčinnosť pri riešení Bezpečnostného incidentu povereným zamestnancom Objednávateľa;
        26. V prípade bezpečnostného kybernetického incidentu Poskytovateľ je povinný využívať formu hlásenia bezpečnostné incidentu , ktorá sa bude riadiť platným predpisom Objednávateľa – „Poriadok o riadení bezpečnostných a kybernetických incidentov Národnej diaľničnej spoločnosti, a.s.“ ako aj postupmi definovanými interných predpisoch Objednávateľa.
        27. Poskytovateľ pri výkone činností dbá na vykonávanie svojich činnosti v súlade s bezpečnostnou dokumentáciou, odporúčaným bezpečnostnými postupmi a v súlade so zásadami due diligence a due care.
  3. Zmluvné strany sa zaväzujú na úprave práv a povinností v oblasti zabezpečenia informačnej a kybernetickej bezpečnosti v spojitosti s poskytovaným predmetom Zmluvy. Poskytovateľ sa zaviaže počas trvania tejto Zmluvy a pri poskytovaní Služieb dodržiavať všetky povinnosti v rozsahu, ktoré sa na Poskytovateľa vzťahujú a ktoré Objednávateľ požaduje.
  4. Poskytovateľ bude súčasne povinný poskytnúť Objednávateľovi maximálnu súčinnosť pri odhaľovaní Kybernetických bezpečnostných incidentov, odstraňovaní a zmierňovaní následkov Kybernetických bezpečnostných incidentov.
  5. Poskytovateľ bude povinný poskytovať Služby prostredníctvom vzdialeného prístupu (za predpokladu, že to povaha týchto prác umožňuje) výlučne po vykonaní príslušného školenia zo strany Objednávateľa a dodržiavania Objednávateľom stanovených podmienok, o ktorých bude Poskytovateľ resp. subdodávateľ (resp. príslušný zamestnanec) oboznámený, čo písomne Objednávateľovi potvrdí.
  6. Poskytovateľ bude povinný zaistiť v dotknutom prostredí Objednávateľa bezpečnostné opatrenia, ktorými sa rozumejú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom bude zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov v priebehu trvania Zmluvy. Bezpečnostné opatrenia realizované v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa budú prijímať s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania služby Objednávateľa. Objednávateľ je za tým účelom povinný poskytnúť Poskytovateľovi súčinnosť a prostredníctvom Odboru riadenia bezpečnosti ako aj Manažéra informačnej a kybernetickej bezpečnosti bude zamestnancom Poskytovateľa a jeho subdodávateľom sprostredkované oboznámenie sa súvisiacou internou bezpečnostnou dokumentáciou. V prípade potvrdeného kybernetického incidentu alebo bezpečnostného incidentu na systémoch na strane Poskytovateľa, sa Poskytovateľ zaväzuje o tejto skutočnosti bezodkladne informovať Objednávateľa a zároveň nahlási kybernetický bezpečnostný incident prostredníctvom e-mailu na adresu: bezpecnostneincidenty@ndsas.sk
  7. Objednávateľ je oprávnený vykonať voči predmetu zákazky a u Objednávateľa ako aj u jeho subdodávateľov audit zameraný na overenie plnenia povinností Poskytovateľa a subdodávateľov podľa tejto a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Poskytovateľa a subdodávateľov na plnenie úloh na úseku bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Poskytovateľa a subdodávateľov pre plnenie cieľov tejto Zmluvy a Objednávateľ sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe.
  8. Objednávateľ sa zaväzuje oznámiť Poskytovateľovi najmenej 15 (pätnásť) pracovných dní vopred svoj zámer realizovať u Poskytovateľa alebo jeho subdodávateľov audit. Vykonanie alebo nevykonanie auditu Objednávateľom, prípadne ním poverenej tretej strany nezbavuje Poskytovateľa zodpovednosti za plnenie povinností Poskytovateľa vyplývajúcich z tejto Zmluvy.
  9. Poskytovateľ bude povinný poskytnúť Objednávateľovi bezpečnostnú dokumentáciu nastavenia a konfigurácie sieťovej komunikácie dotknutého informačného systému v rámci predmetu tejto Zmluvy.
  10. Poskytovateľ bude povinný poskytnúť Objednávateľovi aktualizovanú bezpečnostnú dokumentáciu nastavenia a konfigurácie sieťovej komunikácie dotknutého informačného systému v rámci predmetu tejto Zmluvy pri akejkoľvek významnej zmene systému, ktorá ma vplyv na bezpečnosť systému
  11. V prípade ďalšieho vývoja dotknutých informačných systémov, proces vývoja, testovania, nasadenia a akceptácie musí byť riadený aj z pohľadu bezpečnosti a schválený zástupcami za oblasť bezpečnosti Objednávateľa. Celý proces musí byť  v súlade s platnými postupmi a požiadavkami zákona KB a zákona o ITVS a príslušných vyhlášok.