**Príloha č. 6**

**k zmluve o podpore prevádzky, údržbe a rozvoji informačného systému bezpečnostného monitorovacieho pracoviska Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, č. z.: .....................**

**Rozsah poskytovaných služieb**

**SLUŽBY**

Poskytovateľ v súlade s článkom 3 Zmluvy poskytuje nasledovné služby:

1. Podpora prevádzky a údržba IS SOC podľa bodu 3.2 písm. a)
2. Rozvoj a rozšírenie IS SOC podľa bodu 3.2 písm. b)
3. Školenie používateľov a administrátorov IS SOC podľa bodu 3.2 písm. c)

**Podpora prevádzky a údržba IS SOC podľa bodu 3.2 písm. a)**

1. **Činnosti kategórie 1** realizované počas pracovných dní v čase od 08:00 hod. do 16:00 hod. v priestoroch Objednávateľa prostredníctvom dvoch odborníkov Poskytovateľa a počas pracovných dní v čase od 16:00 hod. do 08:00 hod. a počas sviatkov a dní pracovného pokoja od 00:00 do 24:00 hod. prostredníctvom vzdialeného prístupu minimálne jedným odborníkom Poskytovateľa:

**Zabezpečenie IS SOC operátora:**

* + 1. Sledovanie výstupov dodaných riešení
    2. Vyhodnotenie záznamov a reportov jednotlivých hardvérových a softvérových komponentov dodaného IS SOC
    3. Reakcia na zaznamenané bezpečnostné udalosti a kybernetické bezpečnostné incidenty v IS SOC a bezpečnostné udalosti a kybernetické bezpečnostné incidenty v informačných systémoch Objednávateľa monitorovaných IS SOC (ďalej spolu len „BI“), resp. podozrenia na ich výskyt
    4. Zber všetkých súvisiacich informácií k BI, zabezpečenie stôp (memory dump a pod.)
    5. Aktivovanie dohodnutých postupov pre prijatie nevyhnutných protiopatrení na minimalizáciu dôsledkov BI
    6. Vyhodnotenie získaných informácií, návrhy na zmeny v nastaveniach informačných systémov Objednávateľa monitorovaných IS SOC (ďalej len „IS Objednávateľa“)

**Zabezpečenie ServiceDesk operátora:**

* + 1. Telefonická a emailová dostupnosť pre nahlasovanie požiadaviek používateľov IS Objednávateľa
    2. Zaznamenanie požiadaviek a vloženie do systému
    3. Spracovanie požiadaviek súvisiacich s bezpečnosťou IS Objednávateľa

1. **Činnosti kategórie 2** realizované počas pracovných dní v čase od 08:00 hod. do 16:00 hod. prostredníctvom vzdialeného prístupu minimálne dvoch odborníkov Poskytovateľa a počas pracovných dní v čase od 16:00 hod. do 08:00 hod. a počas sviatkov a dní pracovného pokoja od 00:00 do 24:00 hod. prostredníctvom vzdialeného prístupu minimálne jedného odborníka Poskytovateľa:

**Monitorovanie prevádzky prostredia IS SOC, aktualizácie:**

1. Vyhodnotenie záznamov (logovacie súbory) o prevádzke prostredia (hardvérové (ďalej len „HW“) aj softvérové (ďalej len „SW“) komponenty)
2. Lokalizácia potenciálnych chýb pri používaní IS SOC
3. Optimalizácia prevádzky, aktivovanie dohodnutých postupov riešenia
4. Aktualizácia dokumentácie IS SOC uvedenej v bode 2.1 písm. d) Zmluvy pri zmenách IS SOC
5. Aktualizácia a upgrade HW a SW komponentov IS SOC dohodnutým postupom
6. Kontrola zálohovania, overovanie kvality záloh
7. Neutralizácia chýb

**Konfiguračné úpravy prostredia IS SOC a návrhy úprav IS Objednávateľa:**

* + 1. Analytické práce, odstraňovanie chýb, návrhy na zmeny v nastaveniach IS Objednávateľa
    2. Konfigurácia dodaných súčastí IS SOC
    3. Konfigurácia a správa logovania
    4. Tvorba/úprava parserov a reportov v SIEMe
    5. Správa systémov na orchestráciu a umelú inteligenciu
    6. Správa systému na centralizovaný manažment zraniteľností
    7. Manažment, konfigurácia a testovanie systému Data loss prevention (DLP)
    8. Manažment a konfigurácia systémov pre zber sieťových dát a štatistík
    9. Konfigurácia ServiceDesk systému
    10. Manažovanie riešenia pre zvýšenie bezpečnostného povedomia zamestnancov Objednávateľa (ďalej aj „e-learning“), a to najmä plánovanie modulov e-learningu, nastavovanie rozsahu a obsahu modulov e-learningu, správa oprávnení a podmienok vyhodnocovania
    11. Vykonávanie hardeningu podľa Metodiky zabezpečenia

**Vykonanie zásahu podľa stanoveného času začatia odstraňovania a lehoty na odstránenie chyby podľa prílohy č. 4**

* + 1. Monitorovanie požiadaviek v rámci Informačného systému pre správu požiadaviek
    2. Vyhodnotenie získaných informácií o vzniknutej chybe, stanovenie príčin chyby
    3. V prípade chýb IS SOC návrh optimálneho riešenia chyby
    4. Vyhodnotenie a kvantifikácia nárokov na riešenie vzhľadom na rozsah, náročnosť, dôležitosť a dosah opravy na prevádzku
    5. Výber optimálneho riešenia
    6. Komunikácia a dokumentovanie vybraného riešenia s ohlasovateľom chyby
    7. Oprava chyby vo všetkých častiach IS SOC, ktoré sú chybou dotknuté
    8. Vykonanie modulových testov
    9. Návrh a odsúhlasenie postupu opravy údajov dotknutých chybou
    10. Implementácia dohodnutého postupu
    11. Spracovanie a vytvorenie opravnej konfigurácie IS SOC
    12. Overenie funkčnosti IS SOC po vykonaní zásahu

V prípade nemožnosti plnenia špecifických úloh v rámci činností kategórie 2 prostredníctvom vzdialeného prístupu budú odborníci Poskytovateľa plniť tieto úlohy v priestoroch Objednávateľa.

Aktivity realizované v rámci služieb opravy chýb IS SOC budú pridelené do jednej z troch skupín podľa priority definovaných v prílohe č. 4. Štandardná servisná pohotovosť je zabezpečená v režime dostupnosti 24 hodín denne, 7 dní v týždni. V rámci služby sa vykonávajú zásahy postupom v súlade s prílohou č. 4.

**Rozvoj a rozšírenie IS SOC podľa bodu 3.2 písm. b)**

Službou „Rozvoj a rozšírenie IS SOC“ sa rozumejú komplexné analytické, konfiguračné a implementačné služby vedúce k ďalšiemu rozvoju, rozširovaniu, úpravám funkcionalít, integrácii a upgrade IS SOC. Prostredníctvom tejto služby je možné realizovať aj odbornú činnosť Poskytovateľa týkajúcu sa úpravy IS SOC z dôvodu legislatívnej zmeny, implementáciu komponentov na základe špecifikácií, ktoré doplnia pôvodnú špecifikáciu IS SOC z hľadiska jeho komplexnosti a funkčnosti.

Ide o:

1. implementáciu novej alebo úpravu existujúcej funkčnosti na základe požiadaviek Objednávateľa a legislatívnych zmien,
2. technologický upgrade.

Rozvoj a rozšírenie IS SOC sa uskutočňuje v súlade s bodom 4.5 Zmluvy.

**Školenia používateľov a administrátorov IS SOC podľa bodu 3.2 písm. c)**

Službou „Školenia používateľov a administrátorov IS SOC“ sa rozumejú komplexné služby pre zabezpečenie školení používateľov a administrátorov IS SOC v priestoroch Objednávateľa alebo dištančne (on-line), ak sa tak Zmluvné strany dohodnú; v rámci dohody o dištančnom školení Zmluvné strany dohodnú termín, formu a technické zabezpečenie školenia. Proces zabezpečenia školení je nasledovný:

1. Oprávnená osoba Objednávateľa s dostatočným predstihom zašle Poskytovateľovi písomnú požiadavku na školenie; v požiadavke uvedie špecifikáciu školenia a navrhne termín školenia.
2. Zmluvné strany najneskôr do piatich pracovných dní odo dňa doručenia požiadavky na školenie na spoločnom rokovaní prerokujú a schvália požiadavku na školenie; ak sa Zmluvné strany nedohodnú na termíne školenia, určí termín školenia Objednávateľ.
3. Poskytovateľ vykoná školenie v dohodnutom rozsahu a termíne.
4. Objednávateľ potvrdí prevzatie školenia na odovzdávacom a preberacom protokole podľa prílohy č. 1 Zmluvy. Prílohou faktúry za plnenie podľa bodu 3.2 písm. c) je aj prezenčná listina zo školenia, ak sa realizovalo v priestoroch Objednávateľa.
5. Objednávateľ zabezpečí školiacu miestnosť s potrebným technickým vybavením a dátovou konektivitou, ak sa Zmluvné strany nedohodli na dištančnom školení.
6. Poskytovateľ zabezpečí kvalifikovaného školiteľa spĺňajúceho požiadavky podľa prílohy č. 5, pripraví školiace materiály a vykoná školenie.