**Príloha č. ....**

**Bezpečnostné opatrenia v zmysle požiadaviek zákona o kybernetickej bezpečnosti**

Táto príloha upravuje bezpečnostné opatrenia pre oblasť riadenia dodávateľských služieb, ktoré priamo súvisia s prevádzkou sietí a informačných systémov v zmysle § 20 ods. 3 písm. d) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o kybernetickej bezpečnosti“).

# Riadenie dodávateľských služieb

* 1. Zhotoviteľ/Poskytovateľ, prípadne zamestnanci subdodávateľov Zhotoviteľa/Poskytovateľa (ďalej len „Zhotoviteľ/Poskytovateľ“) sa zaväzuje postupovať v súlade s pracovnoprávnymi predpismi platnými v Slovenskej republike (napr. zákon č. 311/2011 Z. z. Zákonník práce v znení neskorších predpisov, zákon č. 82/2005 Z. z, o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 351/2015 Z. z. o cezhraničnej spolupráci pri vysielaní zamestnancov na výkon prác pri poskytovaní služieb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov), s predpismi v oblasti kybernetickej bezpečnosti (zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov, vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení) a tiež mať splnené všetky povinnosti vyplývajúce z platnej legislatívy, ktoré podmieňujú uzavretie zmluvy (najmä registrácia v registri partnerov verejného sektora a pod.) a v prípade, že Objednávateľovi vzniknú v dôsledku porušenia týchto predpisov zo strany Zhotoviteľa/Poskytovateľa akékoľvek škody, výdavky alebo mu budú uložené sankcie, tieto sa Zhotoviteľ/Poskytovateľ zaväzuje v plnom rozsahu Objednávateľovi zaplatiť. Zmluvné strany sa dohodli, že Objednávateľ je oprávnený započítať tieto škody, výdavky, uložené sankcie voči akýmkoľvek pohľadávkam Zhotoviteľa/Poskytovateľ.

# Školenie v oblasti kybernetickej bezpečnosti

* 1. Objednávateľ sa zaväzuje, po nadobudnutí účinnosti zmluvy, vykonať školenia zamestnancov Zhotoviteľa/Poskytovateľa v oblasti informačnej a kybernetickej bezpečnosti, najmä pre oblasti:

1. technických a organizačných postupov Objednávateľa,
2. realizovaných opatrení Objednávateľa,
3. riadení prístupov k informačným aktívam Objednávateľa,
4. riešení incidentov,
5. riadení rizík,
6. požiadaviek ochrany služieb a informačných aktív Objednávateľa v súvislosti   
   so zabezpečením požadovanej úrovne ich dôverností, integrity a dostupnosti.
   1. O konaní a výsledku každého školenia bude vyhotovený písomný záznam, ktorý bude obsahovať zoznam školených zamestnancov Zhotoviteľa /Poskytovateľa obsah daného školenia.

# Dodržiavanie bezpečnostných politík Objednávateľa

* 1. Zhotoviteľ/Poskytovateľ sa zaväzuje dodržiavať a vyjadruje súhlas s internými predpismi Objednávateľa v oblasti informačnej a kybernetickej bezpečnosti. S obsahom týchto interných predpisov budú zamestnanci Zhotoviteľa/Poskytovateľa oboznámení formou školenia podľa čl. 2 tejto prílohy.

# Ochrana poskytnutých informácií

* 1. Zhotoviteľ/Poskytovateľ sa zaväzuje, že zamestnanci Zhotoviteľa/Poskytovateľa budú počas plnenia zmluvných povinností postupovať tak, aby nebola porušená dôvernosť, integrita a dostupnosť všetkých informácií, ktoré Objednávateľ poskytuje Zhotoviteľovi/Poskytovateľovi.

# Prijímanie a dodržovanie bezpečnostných opatrení Objednávateľa

* 1. Objednávateľ má na ochranu jeho služieb a informačných aktív prijaté a zavedené príslušné technické a organizačné opatrenia. Zhotoviteľ/Poskytovateľ sa zaväzuje dodržiavať a zároveň prijíma všetky interné opatrenia Objednávateľa. Zamestnanci Zhotoviteľa/Poskytovateľa, budú o predmetných opatreniach oboznámení formou školenia podľa čl. 2 tejto prílohy.

# Špecifikácia a rozsah bezpečnostných opatrení prijímaných Zhotoviteľom/Poskytovateľom

* 1. Zhotoviteľ/Poskytovateľ sa zaväzuje prijať a akceptovať bezpečnostné opatrenia Objednávateľa najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona o kybernetickej bezpečnosti nasledovne:
     1. Technické zraniteľnosti systémov:

Zhotoviteľ/Poskytovateľ sa zaväzuje prijať interné opatrenia a nastaviť svoje činnosti spôsobom, ktorý mu umožní systematicky identifikovať a zhromažďovať informácie o zraniteľnostiach a hrozbách, ktoré by mohli mať vplyv na predmet zmluvy, prípadne by prostredníctvom predmetu zmluvy mohli mať vplyv na poskytovanie služby ATM. Zhotoviteľ/Poskytovateľ bude neodkladne informovať Objednávateľa o všetkých zisteniach podľa predchádzajúcej vety. Zároveň sa Zhotoviteľ/Poskytovateľ zaväzuje prijať následné opatrenia, účelom ktorých je minimalizácia rizík vyplývajúcich z identifikovaných hrozieb a zraniteľností ako aj minimalizácia ich opakovania.

* + 1. Riadenie bezpečnosti sietí a informačných systémov

Zhotoviteľ/Poskytovateľ sa zaväzuje prijať a vyslovuje súhlas s internými opatreniami Objednávateľa, ktoré chránia sieťovú komunikáciu a ktoré zabezpečujú spoľahlivý prenos a spracovanie citlivých informácii, tzn. zabezpečujú ich dôvernosť, integritu a dostupnosť. Zhotoviteľ/Poskytovateľ bude o jednotlivých opatreniach Objednávateľa preukázateľne oboznámený prostredníctvom školenia podľa čl. 2 tejto prílohy.

* + 1. Riadenie prístupov

Zhotoviteľ/Poskytovateľ sa zaväzuje prijať a vyslovuje súhlas so všetkými internými opatreniami a požiadavkami Objednávateľa na riadenia prístupov.

* + 1. Riešenie kybernetických bezpečnostných incidentov

Zhotoviteľ/Poskytovateľ sa zaväzuje prijať a vyslovuje súhlas s internými opatreniami a požiadavkami Objednávateľa pre oblasť hlásenia incidentov, najmä opatrenia upravené v čl. 9 tejto prílohy.

* + 1. Monitorovanie, testovanie bezpečnosti a bezpečnostných auditov

Zhotoviteľ/Poskytovateľ sa zaväzuje prijať a vyslovuje súhlas s opatreniami a požiadavkami Objednávateľa pre oblasť monitorovania a kontroly požadovaných stavov bezpečnosti, ktoré sa uskutočňujú najmä prostredníctvom procesov testovania a overovania zariadení (napr. FAT, SAT) a posudzovania bezpečnosti v súlade s prílohou č. 1 Technická špecifikácia Zhotoviteľa/Poskytovateľa.

# Zoznam pracovných rolí

* 1. Zhotoviteľ/Poskytovateľ vedie zoznam jeho zamestnancov, ktorí majú pridelené pracovné role, prostredníctvom ktorých majú prístup k informáciám a údajom Objednávateľa. Zhotoviteľ/Poskytovateľ sprístupní Objednávateľovi zoznam zamestnancov na vyžiadanie alebo pri príležitosti auditu.
  2. Zhotoviteľ/Poskytovateľ je povinný oznámiť Objednávateľovi každú zmenu v personálnom obsadení pracovných rolí podľa bodu 7.1. tohto článku a to zmluvne dohodnutým spôsobom komunikácie.
  3. Všetky osoby, ktoré sa zúčastňujú na predmete plnenia zo strany Zhotoviteľa/Poskytovateľa povinné podpísať vyjadrenie o zachovaní mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti .

# Vykonávanie kontrolných činností a auditu

* 1. Zhotoviteľ/Poskytovateľ je povinný umožniť Objednávateľovi alebo Objednávateľom poverenému audítorovi vykonať u Zhotoviteľa/Poskytovateľa audit alebo kontrolu v oblasti informačnej a kybernetickej bezpečnosti, ktorá môže mať vplyv na predmet zmluvy, prípadne by prostredníctvom predmetu zmluvy mohla mať vplyv na poskytovanie služby ATM, a to za nasledovných podmienok:

1. Objednávateľ je povinný preukázateľne oznámiť požiadavku na vykonanie auditu alebo kontroly týkajúcich sa predmetu zmluvy najneskôr 5 pracovných dní pred plánovaným termínom auditu alebo kontroly,
2. osoby vykonávajúce audit alebo kontrolu sa musia preukázať písomným poverením Objednávateľa na výkon auditu alebo kontroly,
3. osoba vykonávajúca audit/kontrolu je oprávnená vytvárať si kópie dokumentov, súborov a pod. relevantných s ohľadom na predmet zmluvy ,
4. Objednávateľ je povinný o zisteniach auditu alebo kontroly preukázateľne informovať Zhotoviteľa/Poskytovateľa najneskôr do 10 pracovných dní od ukončenia auditu alebo kontroly,
5. Zhotoviteľ/Poskytovateľ je povinný nedostatky identifikované počas auditu alebo kontroly odstrániť na základe harmonogramu dohodnutého medzi Zhotoviteľom/Poskytovateľom a Objednávateľom.

# Hlásenie incidentov

* 1. Zhotoviteľ/Poskytovateľ je povinný, bezodkladne oznámiť Objednávateľovi a riešiť každý incident informačnej a kybernetickej povahy, ktorý má súvis s predmetom zmluvy a mohol ohroziť bezpečnosť softvéru ATM systému a tým mať dopad na bezpečnosť poskytovaných ATM služieb. Hlásenie sa uskutočňuje podľa nasledovných pravidiel:

1. oznámenie musí vykonať bezodkladne,
2. oznámenie musí byť odoslané z jednej z kontaktných elektronických adries Zhotoviteľa/Poskytovateľa na kontaktnú elektronickú adresu Objednávateľa uvedenej v zmluve,
3. oznámenie musí obsahovať tieto informácie:

* opis incidentu a približného odhadu veľkosti a závažnosti incidentu (zoznam dotknutých systémov, funkcionalít systému)
* meno/názov a kontaktné údaje osoby alebo iného kontaktného miesta, kde možno získať viac informácií o incidente,
* dĺžky trvania a opis pravdepodobných následkov incidentu,
* opis Zhotoviteľom/Poskytovateľom navrhovaných a prijatých opatrení s cieľom riešiť incident, prípadne zmierniť jeho dôsledky,
* informáciu o forme a čase ďalšieho hlásenia o stave riešenia incidentu.

# Hlásenie ďalších informácií požadovaných Objednávateľom

* 1. Zhotoviteľ/Poskytovateľ je povinný poskytnúť Objednávateľovi akékoľvek ďalšie, Objednávateľom požadované informácie, ktoré sú potrebné na plnenie povinností Objednávateľa, vyplývajúcich zo všeobecne záväzných právnych predpisov v oblasti kybernetickej bezpečnosti a informácie majúce vplyv na predmet zmluvy.
  2. Hlásenia sa uskutočňujú formou a zmluvne dohodnutým spôsobom komunikácie.

# Licencie a práva

* 1. Zhotoviteľ/Poskytovateľ sa zaväzuje udeliť Objednávateľovi  všetky potrebné práva, licencie a súhlasy podľa ust. § 8 ods. 2 písm. p) vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ktoré sú nevyhnutné na zabezpečenie kontinuity prevádzkovania základnej služby Objednávateľa. Zhotoviteľ/Poskytovateľ udelí práva, licencie a súhlasy podľa prvej vety tohto bodu na dobu nie kratšiu ako päť rokov po skončení zmluvného vzťahu.