ZMLUVA O ZABEZPEČENÍ PLNENIA BEZPEČNOSTNÝCH OPATRENÍ, NOTIFIKAČNÝCH POVINNOSTÍ A OCHRANY OSOBNÝCH ÚDAJOV

uzatvorená v zmysle § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, čl. 28 ods. 3 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (**Všeobecné nariadenie o ochrane osobných údajov**) a § 34 ods. 3 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len ako „**Zmluva**“)
medzi týmito zmluvnými stranami:

Prevádzkovateľ:
Názov: **Hlavné mesto Slovenskej republiky Bratislava**
Sídlo: Primaciálne námestie č. 1, 814 99 Bratislava, Slovenská republika
IČO: 00 603 481
DIČ: 2020372596
IČ DPH: SK2020372596
IBAN:
Zastúpený: Ing. arch. Matúš Vallo, primátor
(ďalej len ako „**Prevádzkovateľ**“ v príslušnom grafickom tvare)

a

Dodávateľ:
obchodné meno:
sídla:
IČO:
DIČ:
IČ DPH:
údaj o zápise v OR
údaj o konajúcej osobe:
(ďalej ako „**Dodávateľ**“ v príslušnom grafickom tvare)

PREAMBULA

Prevádzkovateľ je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**Zákon o kybernetickej bezpečnosti**“).

Základnou službou Prevádzkovateľa sú webové sídlo, elektronické služby a informačné systémy, ktoré sú v zmysle ustanovenia § 3 písm. k) prvého bodu Zákona o kybernetickej bezpečnosti činnosťou v sektore Verejná správa, podsektore Informačné systémy verejnej správy a podľa ustanovenia § 17 ods. 2 písm. b) Zákona o kybernetickej bezpečnosti sú zaradené do zoznamu základných služieb.

Dodávateľ je zmluvným partnerom Prevádzkovateľa na výkon činností, ktoré priamo súvisia s prevádzkou elektronických komunikačných sietí (ďalej len „**Siete**“) a informačných systémov Prevádzkovateľa, pričom tieto činnosti Dodávateľ uskutočňuje na základe Zmluvy o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania, uzatvorenej s Prevádzkovateľom dňa _____ (ďalej len „**Základný kontrakt**“).

Dodávateľ je pri výkone činností podľa predchádzajúceho odseku Prevádzkovateľom poverený na spracúvanie osobných údajov v súlade so špecifikáciou spracúvania osobných údajov uvedenej v Prílohe č. 5 tejto Zmluvy.

Dodávateľ vyhlasuje, že je odborne spôsobilý na plnenie predmetu tejto Zmluvy, má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto zmluvy. Súčasne vyhlasuje, že prijal primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky Všeobecného nariadenia o ochrane údajov a aby sa zabezpečila ochrana práv dotknutej osoby.

Ak nie je uvedené inak, pojmy používané v tejto Zmluve majú význam im priradený v Zákone o kybernetickej bezpečnosti, jeho vykonávacích predpisoch, Všeobecnom nariadení o ochrane osobných údajov a iných predpisoch v oblasti ochrany osobných údajov.

Článok I.
Predmet Zmluvy

1. Predmetom tejto Zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa.
2. Predmetom tejto Zmluvy je špecifikácia spracúvania osobných údajov a úprava práv a povinností zmluvných strán na úseku ochrany osobných údajov.
3. Táto Zmluva upravuje základné princípy spolupráce zmluvných strán pri uskutočňovaní plnenia bezpečnostných opatrení – úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa počas ich životného cyklu, s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby Prevádzkovateľa a na porušenia ochrany osobných údajov (ďalej len „**Ciele**“).
4. Súčasťou záväzkov Dodávateľa podľa tejto Zmluvy je povinnosť Dodávateľa prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti a ochrany osobných údajov v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené Ciele tejto Zmluvy. Prevádzkovateľ vyhlasuje, že súhlasí so špecifikáciou a rozsahom bezpečnostných opatrení prijímaných Dodávateľom v zmysle tejto Zmluvy. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
5. Dodávateľ sa na základe tejto Zmluvy zároveň zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa, s ktorými ho Prevádzkovateľ oboznámil. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa. Dodávateľ súčasne akceptuje, že bezpečnostné politiky Prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu Sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa a ochranu osobných údajov.
6. Na základe tejto Zmluvy sa tiež Dodávateľ zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti a ochrany osobných údajov v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené jej Ciele.
7. Odplata za plnenie povinností Dodávateľa podľa tejto Zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto Zmluvy sú v celom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa Základného kontraktu a za plnenie povinností podľa tejto Zmluvy Dodávateľ nemá nárok na žiadne ďalšie peňažné plnenia od Prevádzkovateľa.
8. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto Zmluvy po celú dobu trvania Základného kontraktu.

Článok II.
Prevencia kybernetických bezpečnostných incidentov

1. Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti Siete a informačného systému alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť Prevádzkovateľa alebo ktorej následkom je:
   a) strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému Prevádzkovateľa,
   b) obmedzenie alebo odmietnutie dostupnosti základnej služby Prevádzkovateľa,
   c) vysoká pravdepodobnosť kompromitácie činností základnej služby Prevádzkovateľa alebo
   d) ohrozenie bezpečnosti informácií Prevádzkovateľa.
2. Incident definovaný v čl. I. Základného kontraktu sa považuje sa kybernetický bezpečnostný incident v zmysle tejto Zmluvy, okrem nekritického incidentu, ktorý nespôsobuje výpadok služby ani iné následky podľa čl. II ods. 1. písm. a) až d) tejto Zmluvy.
3. Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa a bezpečnosti spracúvania osobných údajov (ďalej len „**Incidenty**"):
   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez Dodávateľa nebolo možné zasiahnuť Siete a informačné systémy Prevádzkovateľa;
   b) prijať primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti spracúvania osobných údajov, najmä pseudonymizáciu a šifrovanie osobných údajov; schopnosť zabezpečiť trvalú dôvernosť,

integritu, dostupnosť a odolnosť systémov spracúvania a služieb; schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade Incidentu; proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov;

c) sledovať výstrahy, varovania, ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov Incidentov, tieto vyhodnocovať a vykonať protiopatrenia v záujme ochrany oprávnených záujmov Prevádzkovateľa;
d) prijímať od Prevádzkovateľa varovania pred Incidentmi;
e) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa;
f) vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa alebo kybernetickú bezpečnosť Sietí a informačných systémov Prevádzkovateľa alebo ochranu osobných údajov;
g) predchádzať vzniku Incidentov;
h) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o Incidentoch;
i) zasielať Prevádzkovateľovi včasné varovania pred Incidentmi, o ktorých sa dozvie vlastnou činnosťou podľa tejto Zmluvy alebo iným spôsobom;
j) informovať Prevádzkovateľa o Incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti;
k) podávať Prevádzkovateľovi oznámenia, že došlo k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k riziku pre práva a slobody fyzických osôb bez zbytočného odkladu potom, čo sa o porušení ochrany osobných údajov dozvedel;
l) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa v rozsahu Základného kontraktu,
m) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov podieľajúcich sa na plnení základného kontraktu a/alebo tejto zmluvy a/alebo majúcich prístup k informáciám a údajom Prevádzkovateľa.

4. Dodávateľ je povinný mať počas trvania tejto Zmluvy také technické, technologické a personálne vybavenie, ktoré je potrebné na riadne a včasné plnenie tejto Zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti v rozsahu potrebnom na efektívne napĺňanie Cieľov tejto Zmluvy.
5. Neoddeliteľnými prílohami tejto Zmluvy sú:
   a) rozsah činnosti Dodávateľa v zmysle Základného kontraktu (Príloha č. 1),
   b) špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma Dodávateľ a s ktorými súhlasí (Príloha č. 2),
   c) zoznam pracovných rolí Dodávateľa, ktoré majú mať prístup k informáciám a údajom Prevádzkovateľa a zoznam zamestnancov Dodávateľa a iných osôb, podieľajúcich sa za Dodávateľa na plnení Základného kontraktu a/alebo tejto Zmluvy a/alebo majúcich prístup k informáciám a údajom Prevádzkovateľa (Príloha č. 3),
   d) zoznam Dodávateľom navrhnutých a Prevádzkovateľom schválených Subdodávateľov (Príloha č. 4),
   e) špecifikácia spracúvania osobných údajov (Príloha č. 5).
6. **<u>Dodávateľ je povinný bezodkladne oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí Dodávateľa.</u>**
7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností a všetky potrebné informácie na preukázanie splnenia povinností podľa tejto Zmluvy v bezpečnostnej dokumentácii a dokumentácii na úseku ochrany osobných údajov, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi na nahliadnutie a zhotovenie kópií.
8. Dodávateľ je povinný prijať a dodržiavať všeobecné a sektorové bezpečnostné opatrenia v dotknutých oblastiach podľa Zákona o kybernetickej bezpečnosti a 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, najmenej pre oblasť podľa § 20 ods. 3 písm. b), až h), j), k), m) Zákona o kybernetickej bezpečnosti, v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa a Prílohy k vyhláške Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov, ktorá upravuje opatrenia na elimináciu rizík pre práva fyzickej osoby a Prílohy 2 k vyhláške Úradu podpredsedu vlády SR pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Článok III.
Reaktivita pri hlásení Incidentov

1. Dodávateľ je povinný Prevádzkovateľovi bezodkladne hlásiť každý Incident spôsobom určeným Prevádzkovateľom, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie Incidentov. Ak do okamihu hlásenia Incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie Incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky Siete a informačného systému toto hlásenie doplní.
2. Pri incidentoch definovaných v čl. I Základného kontraktu Dodávateľ postupuje v súlade s čl. VIII Základného kontraktu a touto Zmluvou.
3. Dodávateľ je povinný riešiť Incident najmä odozvou alebo inou reakciou na Incident, ohraničením Incidentu a jeho dopadov, nápravou následkov Incidentu, asistenciou pri riešení Incidentu na mieste, reakciou na Incident a podporou reakcií na Incident (ďalej len **„Reaktívne opatrenie").** Pri riešení Incidentu je Dodávateľ povinný na žiadosť Prevádzkovateľa spolupracovať s Prevádzkovateľom, Národným bezpečnostným úradom a Ministerstvom pre investície a informatizáciu Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie Incidentu.
4. Dodávateľ je povinný Prevádzkovateľovi bezodkladne oznámiť a preukázať vykonanie Reaktívneho opatrenia a jeho výsledok.
5. Dodávateľ je povinný v čase Incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní, a poskytnúť ho Prevádzkovateľovi.
6. Dodávateľ je povinný Prevádzkovateľovi oznámiť skutočnosť, že v súvislosti s Incidentom došlo k porušeniu ochrany osobných údajov a súčasne poskytnúť mu súčinnosť pri plnení jeho povinností pri oznamovaní týchto porušení dozornému orgánu a dotknutým osobám.
7. Dodávateľ je povinný Prevádzkovateľovi oznámiť skutočnosť, že v súvislosti s Incidentom mohlo dôjsť k spáchaniu trestného činu.
8. Po vyriešení Incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu Incidentu (ďalej len „**ochranné opatrenia**") na schválenie. Ak dodávateľ nenavrhne ochranné opatrenia v určenej lehote alebo ak sú navrhované ochranné opatrenia zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom na jeho návrhu.
9. Po schválení ochranných opatrení Prevádzkovateľom je Dodávateľ povinný ochranné opatrenia bez zbytočného odkladu vykonať.
10. Po vykonaní ochranných opatrení Dodávateľom je Dodávateľ povinný preveriť ich účinnosť.

Článok IV.
Spracúvanie osobných údajov

1. Dodávateľ je oprávnený pri výkone činností podľa Základného kontraktu spracúvať osobné údaje len na základe pokynov Prevádzkovateľa uvedených v Základnom kontrakte a v tejto Zmluve.
2. Dodávateľ je povinný spracúvať osobné údaje v súlade so Všeobecným nariadením o ochrane údajov a súvisiacimi právnymi predpismi.
3. Dodávateľ v čo najväčšej miere pomáha Prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinností reagovať na žiadosti o výkon práv dotknutej osoby.
4. Dodávateľ je povinný vytvoriť systém na vybavovanie žiadostí o výkon práv dotknutých osôb. Pokiaľ je Dodávateľovi doručená žiadosť dotknutej osoby, bez zbytočného odkladu ju odstúpi Prevádzkovateľovi, pokiaľ sa spracúvanie jej osobných údajov týka Základného kontraktu alebo tejto Zmluvy.
5. Dodávateľ bezodkladne informuje Prevádzkovateľa, ak sa podľa jeho názoru pokynom porušuje Všeobecné nariadenie na ochranu osobných údajov alebo iné súvisiace právne predpisy.

Článok V.
Ochrana informácií a povinnosť zachovávať mlčanlivosť

1. Dodávateľ je povinný chrániť všetky informácie poskytnuté mu Prevádzkovateľom. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa.
2. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením tejto Zmluvy a/alebo Základného kontraktu 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.
3. Dodávateľ je povinný zabezpečiť, aby každá osoba zúčastnená na predmete plnenia Základného kontraktu a/alebo tejto Zmluvy za Dodávateľa neodkladne podpísala vyhlásenie o zachovávaní mlčanlivosti o skutočnostiach, o

ktorých sa dozvedela v súvislosti s plnením úloh podľa Zákona o kybernetickej bezpečnosti a ktoré nie sú verejne známe. Rovnako je povinný zabezpečiť, aby každá osoba oprávnená spracúvať osobné údaje v jeho mene bola zaviazaná, že zachová dôvernosť informácií. Dodávateľ je v rámci toho povinný zabezpečiť trvalé zachovávanie mlčanlivosti o všetkých takýchto skutočnostiach každou z týchto osôb, a to aj po skončení plnenia predmetu Zmluvy a/alebo predmetu Základného kontraktu.

Článok VI.
Spôsob a forma hlásenia ďalších informácií požadovaných Prevádzkovateľom na plnenie jeho povinností vyplývajúcich zo Zákona o kybernetickej bezpečnosti a ich vymedzenie, kontaktné osoby na úseku kybernetickej bezpečnosti

1. Dodávateľ je povinný hlásiť Prevádzkovateľovi za účelom plnenia povinností Prevádzkovateľa vyplývajúcich zo Zákona o kybernetickej bezpečnosti všetky ďalšie Prevádzkovateľom požadované informácie, najmä informácie potrebné pre:
   a) riešenie kybernetického bezpečnostného incidentu,
   b) hlásenie závažného kybernetického incidentu,
   c) poskytnutie súčinnosti a spolupráce s Národným bezpečnostným úradom,
   d) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
   e) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka.
2. Dodávateľ je povinný realizovať hlásenia podľa ods. 1. tohto článku Zmluvy a komunikovať s Prevádzkovateľom pri plnení povinností podľa tejto Zmluvy spôsobom a formou určeným Prevádzkovateľom, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií. Zmluvné strany berú na vedomie, že hlásenia podľa ods. 1. tohto článku Zmluvy ako aj poskytovanie ďalších informácií pri plnení povinností podľa tejto Zmluvy si budú realizovať telefonicky, e-mailom a/alebo písomne, pričom konkrétny spôsob a formu takého oznámenia budú voliť podľa hľadiska účelnosti a naliehavosti nahlasovaných informácií.
3. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:
   meno a priezvisko: _____
   funkcia/pracovná pozícia _____
   telefónne číslo: _____
   e-mailová adresa: _____
4. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti:
   meno a priezvisko: _____
   funkcia/pracovná pozícia _____
   telefónne číslo: _____
   e-mailová adresa: _____
5. Zmenu kontaktných osôb na úseku kybernetickej bezpečnosti môže každá zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok VII.
Spôsob a forma hlásenia ďalších informácií požadovaných Prevádzkovateľom na plnenie jeho povinností vyplývajúcich zo Všeobecného nariadenia o ochrane údajov, kontaktné osoby na úseku ochrany osobných údajov

1. Dodávateľ je povinný hlásiť Prevádzkovateľovi za účelom plnenia povinností Prevádzkovateľa vyplývajúcich zo Všeobecného nariadenia o ochrane osobných údajov všetky ďalšie Prevádzkovateľom požadované informácie, najmä informácie potrebné pre:
   a) oznámenie porušenia ochrany osobných údajov dozornému orgánu,
   b) oznámenie porušenia ochrany osobných údajov dotknutej osobe,
   c) výkon práv dotknutých osôb,
   d) poskytnutie súčinnosti a spolupráce s Úradom na ochranu osobných údajov SR,
   e) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v súdnom konaní,
   f) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa porušenie ochrany osobných údajov týka.
2. Oznámenie podľa ods. 1 tohto článku musí obsahovať aspoň:

a) opis povahy porušenia ochrany osobných údajov vrátane kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
d) opis opatrení prijatých alebo navrhovaných Dodávateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

3. V rozsahu, v akom nie je možné poskytnúť informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.
4. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku ochrany osobných údajov:
   meno a priezvisko: _____
   funkcia/pracovná pozícia _____
   telefónne číslo: _____
   e-mailová adresa: _____
5. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku ochrany osobných údajov:
   meno a priezvisko: _____
   funkcia/pracovná pozícia _____
   telefónne číslo: _____
   e-mailová adresa: _____
6. Zmenu kontaktných osôb na úseku ochrany osobných údajov môže každá zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok VIII.
Podmienky a možnosti zapojenia ďalšieho Dodávateľa

1. Dodávateľ môže za účelom plnenia svojho záväzku podľa Základného kontraktu ustanoviť ďalšieho Dodávateľa (ďalej len „**Subdodávateľ**“), ktorý bude úplne alebo čiastočne zabezpečovať plnenie pre Prevádzkovateľa namiesto Dodávateľa, avšak za splnenia nasledovných podmienok:
   a) Dodávateľ môže ustanoviť Subdodávateľa iba na základe predchádzajúceho písomného súhlasu Prevádzkovateľa; Dodávateľ v žiadosti o udelenie súhlasu písomne oznámi Prevádzkovateľovi obchodné meno a ostatné identifikačné údaje Subdodávateľa,
   b) Dodávateľ je povinný zmluvne zaviazať Subdodávateľa k plneniu povinností podľa Základného kontraktu a tejto Zmluvy, a uložiť mu rovnaké povinnosti týkajúce sa plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa, ako sú ustanovené v tejto Zmluve, uložiť mu povinnosť poskytnutia dostatočných záruk na vykonanie primeraných technických opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky všeobecného nariadenia na ochranu osobných údajov,
   c) zodpovednosť voči Prevádzkovateľovi nesie Dodávateľ, ak Subdodávateľ nesplní svoje povinnosti týkajúce Základného kontraktu a tejto Zmluvy; tým nie je dotknutý nárok Dodávateľa na náhradu škody voči Subdodávateľovi.

Článok IX.
Spoločné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto Zmluvy v súlade so Zákonom o kybernetickej bezpečnosti, a inými zákonnými úpravami, vykonávacími predpismi 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. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto Zmluvy v súlade so sektorovými bezpečnostnými opatreniami (§ 32 ods. 2 Zákona o kybernetickej bezpečnosti), ktoré vydáva Ministerstvo pre investície a informatizáciu Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.

3. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
4. Dodávateľ je povinný mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy, v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
5. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto Zmluvy (evidovanie logov a Incidentov a dokumentovanie školení svojich zamestnancov – prezenčné listiny) a na žiadosť Prevádzkovateľa mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
6. Dodávateľ je oprávnený plniť Základný kontrakt pre Prevádzkovateľa prostredníctvom svojich Subdodávateľov čiastočne v nevyhnutnom rozsahu v prípade, že toto plnenie priamo súvisí s prevádzkou Sietí a informačných systémov Prevádzkovateľa, pričom je povinný zabezpečiť riadne plnenie povinností na úseku kybernetickej bezpečnosti v rozsahu Zákona o kybernetickej bezpečnosti.. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať kontrolné činnosti a audit v súlade s ustanoveniami čl. XI. tejto zmluvy aj u takýchto Subdodávateľov, zabezpečujúcich úplne alebo čiastočne plnenie Základného kontraktu pre Prevádzkovateľa namiesto Dodávateľa.
7. Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto Zmluvy ohrozuje plnenie Cieľov tejto Zmluvy, pričom za dôsledky Incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Dodávateľa podľa tejto Zmluvy neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá Prevádzkovateľovi v plnom rozsahu.

Článok X.
Trvanie a zánik Zmluvy, sankčný mechanizmus

1. Táto Zmluva sa uzatvára na dobu určitú, odo dňa jej uzatvorenia do konca trvania Základného kontraktu definovaného podľa preambuly v ods. 3 tejto Zmluvy.
2. Zmluvný vzťah na základe tejto Zmluvy zanikne súčasne so zánikom Základného kontraktu.
3. Túto Zmluvu je možné ukončiť vždy dohodou zmluvných strán o skončení trvania Zmluvy, a to ku dňu uvedenému v takej dohode.
4. Prevádzkovateľ je oprávnený od tejto Zmluvy písomne odstúpiť v prípadoch, ak Dodávateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy. Možnosť ktorejkoľvek zmluvnej strany odstúpiť od tejto zmluvy zo zákonom ustanovených dôvodov týmto nie je dotknutá.
5. Zánik tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto Zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy, ku ktorému dôjde do jej zániku.
6. V prípade každého jednotlivého porušenia ktorejkoľvek povinnosti Dodávateľa, vyplývajúcej z tejto Zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 5.000,-EUR (slovami: tisíc Euro).
7. V prípade opakovaného porušenia identickej povinnosti Dodávateľa, vyplývajúcej z tejto zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 1.000,-EUR (slovami: tisíc Euro).
8. Ustanovenia o zmluvných sankciách uvedených v Základnom kontrakte týmto nie sú dotknuté.
9. Zmluvná pokuta je splatná na základe výzvy Prevádzkovateľa na zaplatenie zmluvnej pokuty v lehote 30 (tridsať) dní odo dňa jej doručenia Dodávateľovi.
10. Nárok Prevádzkovateľa na náhradu škody voči Dodávateľovi, aj vo výške presahujúcej zmluvnú pokutu, nie je ustanoveniami o dojednaní zmluvnej pokuty, uplatnením zmluvnej pokuty voči Dodávateľovi ani jej zaplatením Dodávateľom dotknutý.
11. Ak vznikne Prevádzkovateľovi ujma z dôvodu pochybenia Dodávateľa, ktorý poruší svoje povinnosti dojednané touto Zmluvou alebo uložené mu právnymi predpismi, a to tak, že Prevádzkovateľ bude na základe alebo v súvislosti s takou skutočnosťou zodpovedný za správny delikt v oblasti kybernetickej bezpečnosti alebo ochrany osobných údajov, vzniká Prevádzkovateľovi nárok na náhradu takejto ujmy voči Dodávateľovi v plnom rozsahu, vrátane prípadných ďalších vynaložených nákladov, vrátane nákladov za právne zastúpenie.

Článok XI.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu kybernetickej bezpečnosti a ochrany osobných údajov u Dodávateľa Prevádzkovateľom

1. Prevádzkovateľ je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti a ochrany osobných údajov, ako aj

nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy.

2. Prevádzkovateľ je oprávnený realizovať audit u Dodávateľa sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu uskutočňuje taká Prevádzkovateľom poverená tretia osoba.
3. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti a ochrany osobných údajov podľa tejto Zmluvy.
4. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky osobám, ktoré sa za Dodávateľa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti a ochrany osobných údajov podľa tejto Zmluvy.
5. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad plnenia povinností Dodávateľom s touto Zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti a ochrany osobných údajov podľa tejto Zmluvy, aktuálne bezpečnostné povedomie svojich zamestnancov a iných osôb zúčastnených na predmete plnenia Základného kontraktu a/alebo tejto Zmluvy za Dodávateľa, ich záväzok a poučenie o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
6. Prevádzkovateľ je povinný oznámiť Dodávateľovi svoj zámer realizovať u Dodávateľa audit najmenej 14 pracovných dní vopred.
7. Výsledok auditu Prevádzkovateľ zaznamená do zápisnice. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 30 kalendárnych dní.
8. Ak Dodávateľ neumožní Prevádzkovateľovi, resp. Prevádzkovateľom poverenej tretej osobe, bezdôvodne vykonanie auditu ani po opakovanej písomnej výzve, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti a/alebo ochrany osobných údajov podľa tejto Zmluvy.
9. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto Zmluvy.
10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu u Dodávateľa a ktoré nie sú verejne známe. Prevádzkovateľ je povinný zabezpečiť zachovávanie mlčanlivosti v tomto zmysle každou osobou zúčastnenou na audite u Dodávateľa. Povinnosť zachovávať mlčanlivosť trvá aj po skončení trvania tejto Zmluvy a/alebo Základného kontraktu.
11. Prevádzkovateľ a ním poverené osoby pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa 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 musia byť Dodávateľom oboznámení v zmysle nasledujúcich ustanovení tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne informovať Prevádzkovateľa a ním poverené osoby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ 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 Dodávateľa.

Článok XII.
Záverečné ustanovenia

1. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto Zmluvy Prevádzkovateľovi udelí, poskytne, prevedie alebo na Prevádzkovateľa postúpi všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu s Prevádzkovateľom založeného touto Zmluvou po dobu dohodnutú v trvaní päť rokov po ukončení zmluvného vzťahu.
2. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto Zmluvy Prevádzkovateľovi vráti, prevedie a podľa pokynov Prevádzkovateľa prípadne aj zničí všetky informácie a osobné údaje vrátane ich kópií, ku ktorým mal Dodávateľ počas trvania zmluvného vzťahu prístup.
3. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto Zmluvy a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na plnenie predmetu tejto Zmluvy.
4. Dodávateľ bez predchádzajúceho písomného súhlasu Prevádzkovateľa nemá právo previesť práva a povinnosti vyplývajúce z tejto Zmluvy na tretiu osobu.

5. Táto Zmluva predstavuje úplnú dohodu zmluvných strán týkajúcu sa predmetu tejto Zmluvy a nahrádza v celom rozsahu akékoľvek predchádzajúce dohody či návrhy uvádzané v korešpondencii či na rokovaniach, či už ústne alebo písomné, ku ktorým došlo pred uzatvorením tejto Zmluvy a ktoré jej uzatvorením zanikajú.
6. Táto Zmluva sa riadi právom Slovenskej republiky. Právne vzťahy neupravené touto Zmluvou sa spravujú príslušnými ustanoveniami Obchodného zákonníka a ostatnými všeobecne záväznými právnymi predpismi. Na riešenie sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.
7. Zmluva je vyhotovená v štyroch vyhotoveniach, ktoré majú povahu originálu, po dvoch vyhotoveniach pre každú zmluvnú stranu.
8. Neoddeliteľnou súčasťou tejto Zmluvy sú jej prílohy v zmysle ustanovenia čl. II, bodu 3. tejto Zmluvy.
9. Akúkoľvek zmenu alebo doplnenie tejto Zmluvy je možné vykonať výlučne formou písomných dodatkov podpísaných oboma zmluvnými stranami.
10. Táto Zmluva je uzatvorená, vzniká a zaväzuje zmluvné strany okamihom, keď je podpísaná oboma zmluvnými stranami.
11. Osoby konajúce za zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, prejav ich vôle je slobodný a vážny, určitý a zrozumiteľný a je plne v súlade s obsahom tejto zmluvy, zmluvná voľnosť zmluvných strán nie je obmedzená, Zmluvu si pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom ju vlastnoručne podpísali.

V _____, dňa _____ V _____, dňa _____

za Prevádzkovateľa za Dodávateľa

_____ _____

Príloha č. 1 – Rozsah činností Dodávateľa v zmysle Základného kontraktu
Príloha č. 2 – Špecifikácia a rozsah bezpečnostných opatrení
Príloha č. 3 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa v zmysle Základného kontraktu
Príloha č. 4 - Zoznam schválených Subdodávateľov
Príloha č. 5 - Špecifikácia spracúvania osobných údajov

PRÍLOHA 1
Rozsah činností Dodávateľa v zmysle Základného kontraktu

Predmetom Základného kontaktu je vytvorenie mobilnej aplikácie na zabezpečenie:

- bezproblémovej, časovo a administratívnej efektívnej úhrady parkovného zákazníkmi Prevádzkovateľa,
- kontroly úhrady parkovného na základe integrácie aplikácie do systému ParkSys.

Dodávateľ aplikáciu vytvorí, otestuje a integruje do systému ParkSys v súlade s požiadavkami Prevádzkovateľa uvedenými v Základnom kontrakte.

Dodávateľ je v zmysle Základného kontraktu povinný:

- umožniť zákazníkovi Prevádzkovateľa bezodplatne inštalovať aplikáciu do mobilného zariadenia zákazníka;
- umožniť prostredníctvom aplikácie vyhľadanie parkovacieho miesta,
- zabezpečiť zákazníkovi Prevádzkovateľa prostredníctvom aplikácie bezpečné pripojenie na platobný systém banky a umožniť zaplatiť parkovné prostredníctvom platobnej karty na zberný účet Prevádzkovateľa;
- zabezpečiť bezpečné spracovanie osobných údajov zákazníkov Prevádzkovateľa v súvislosti s plnením Základného kontraktu,
- zabezpečiť poskytnutie zjednodušenej faktúry podľa § 74 ods. 3 písm. a) zákona o DPH zákazníkovi Prevádzkovateľa v mene Prevádzkovateľa ku každej úhrade parkovného;
- prostredníctvom aplikácie upozorniť zákazníka Prevádzkovateľa na to, že sa mu končí doba, za ktorú má zaplatené parkovné;
- zabezpečiť zákazníkovi Prevádzkovateľa možnosť prostredníctvom aplikácie predĺžiť dobu užívania parkovacieho miesta.

PRÍLOHA 2
Špecifikácia a rozsah bezpečnostných opatrení

A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

1. Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre Dodávateľa záväzný a obsahuje najmenej
   a) určenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,
   b) základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré Dodávateľ má zavedené a riadi sa nimi v oblastiach:
      - organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
      - riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
      - personálna bezpečnosť,
      - riadenie prístupov,
      - riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami,
      - bezpečnosť pri prevádzke informačných systémov a sietí,
      - hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
      - ochrana proti škodlivému kódu,
      - sieťová a komunikačná bezpečnosť,
      - akvizícia, vývoj a údržba informačných technológií,
      - zaznamenávanie udalostí a monitorovanie,
      - riadenie kontinuity procesov. fyzická bezpečnosť a bezpečnosť prostredia,
      - riešenie kybernetických bezpečnostných incidentov,
      - kryptografické opatrenia,
      - kontinuita prevádzky informačných technológií,
      - audit a kontrolné činnosti.

B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:
1. Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Návrh a prijatie bezpečnostných opatrení.
3. Periodické preskúmavanie rizík.
   a) Identifikácia všetkých významných informačných aktív Dodávateľa a určenie ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.
   b) Zaradenie informačných aktív podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných stupňov, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.
   c) Vypracovanie a implementácia interného riadiaceho aktu na riadenie bezpečnostných rizík, ktorý obsahuje najmenej:
      - zodpovednosť za vykonanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
      - proces vykonávania analýzy rizík,
      - maticu určenia závažnosti rizika,
      - periodicitu vykonávania analýzy rizík,
      - spôsob dokumentácie bezpečnostných rizík a prijatých opatrení a postupov na ich zníženie na prijateľnú úroveň v podľa matice určenia závažnosti rizika.
4. Vykonávanie analýzy rizík najmenej raz za rok.
5. Vytvorenie a udržiavanie zoznamu informačných aktív.

C. Personálna bezpečnosť

1. Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.
2. Dodávateľ zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.

3. Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
4. Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí:
   a) vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
   b) zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
   c) zrušenie prístupových práv v informačných systémoch verejnej správy,
   d) odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.
5. Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
6. Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.
7. Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov, najmä:
   a) prideľovanie prístupových práv,
   b) zásady tvorby a používania hesiel,
   c) zásady ochrany pred infiltráciou škodlivým kódom,
   d) zásady bezpečného používania elektronickej pošty,
   e) zásady bezpečného používania internetu,
   f) zásady bezpečného používania komunikačných nástrojov a sociálnych sietí,
   g) zásady používania prenosných zariadení a médií,
   h) zálohovanie údajov,
   i) riešenie kybernetických bezpečnostných incidentov,
   j) ochranu fyzického majetku,
   k) pohyb v priestoroch Dodávateľa.
8. Zavedenie procesu preukázateľného poučenia a oboznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.
9. Zavedenie procesu preukázateľného oboznámenia správcov informačných technológií verejnej správy s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.
10. Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oboznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, ako aj opatreniami a postupmi zavedenými v organizácii správcu na ich elimináciu najmenej raz za rok.
11. Na prístup k informačným technológiám verejnej správy sa vyžaduje:
   a) oboznámenie so spôsobom používania informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy v rozsahu svojej pracovnej náplne,
   b) poučenie na rozoznanie kybernetického bezpečnostného incidentu od bežnej prevádzky a zvládnutie postupu pri kybernetickom bezpečnostnom incidente,
   c) oboznámenie so zamestnancom, na ktorého je možné sa obracať s otázkami a nejasnosťami pri používaní informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy.

D. Riadenie prístupov

1. Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií verejnej správy.
2. Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy.
3. Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok.
4. Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií verejnej správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.
5. Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.
6. Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.
7. Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.

8. Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá umožní používateľom najmä:
   a) zabezpečiť absolútnu kontrolu nad heslom svojho používateľského účtu,
   b) presadzovať určenú štruktúru hesla,
   c) vyžadovať pravidelnú zmenu hesla,
   d) uchovávať a prenášať používateľské heslá bezpečným spôsobom.
9. Zabezpečenie formálneho riadenia a autorizácie prideľovania privilegovaných prístupov do informačných technológií verejnej správy a ich obmedzenie len na nevyhnutné prípady.
10. Preskúmavanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za rok.
11. Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií verejnej správy a na prácu na diaľku.
12. Automatické zaznamenávanie každého prístupu administrátora do informačných technológií verejnej správy a automatické zaznamenávanie prístupu používateľa.
13. Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií verejnej správy.
14. Implementácia centrálnej správy identít (IDM).
15. Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok.
16. Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť mesiacov.
17. Implementácia, vynucovanie prístupových rolí v informačných technológiách verejnej správy.
18. Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov šesť mesiacov.

E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami

1. V zmluve so Subdodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Požiadavky v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií verejnej správy.
3. Zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahujú najmenej záväzok:
   a) plnenia určených požiadaviek a kritérií pre oblasť kybernetickej bezpečnosti a informačnej bezpečnosti pri dodávke predmetu zmluvy,
   b) ochrany informácií, ku ktorým je poskytnutý prístup,
   c) oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti a ďalších opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti špecifických na plnenie predmetu Základného kontraktu a tejto Zmluvy,
   d) riadenia a monitorovania prístupov do informačných technológií verejnej správy vrátane spôsobu a mechanizmu,
   e) možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
   f) oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií verejnej správy zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,
   g) spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
   h) zachovania úrovne kybernetickej bezpečnosti a informačnej bezpečnosti pri významných zmenách vrátane spôsobu a formy prechodu k inému Subdodávateľovi.
4. Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti a posúdia sa najmä
   a) kritické komponenty a prvky služby,
   b) možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
   c) možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch medzi Dodávateľom a Subdodávateľmi,
   d) ďalšie možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému Subdodávateľovi.
5. Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti.

6. Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia kybernetickej bezpečnosti a informačnej bezpečnosti Dodávateľa.
7. Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.
8. Pre informačné technológie verejnej správy, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.
9. Interný predpis ustanovujúci zásady kybernetickej bezpečnosti a informačnej bezpečnosti pre Subdodávateľov a tretie strany obsahuje najmenej bezpečnostné požiadavky:
   a) pri riadení vzťahov so Subdodávateľmi,
   b) pri ošetrení kybernetickej bezpečnosti a informačnej bezpečnosti v zmluvách so Subdodávateľmi,
   c) dodávateľských reťazcov informačných technológií verejnej správy,
   d) monitorovania a preskúmavania dodávateľských služieb,
   e) riadenia zmien v službách Subdodávateľa,
   f) na prístupové práva a účty,
   g) na fyzickú bezpečnosť,
   h) na ochranu a zálohovanie dát,
   i) na mobilné prostriedky a vzdialený prístup.
10. Vytvorenie a využívanie procesu pravidelného monitorovania a preskúmavania kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu so Subdodávateľmi.

F. Bezpečnosť pri prevádzke informačných systémov a sietí

1. Na účinnú prevenciu pred stratou dát u Dodávateľa sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru.
2. Dodávateľ vypracuje a dodržiava politiku zálohovania, ktorá definuje požiadavky Prevádzkovateľa na zálohovanie vrátane doby uchovávania, testovania záloh, ako aj opatrenia na ochranu záložných médií.
3. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykateľného priestoru.
4. Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách.
5. Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.
6. Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok.
7. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.
8. Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú.
9. Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.
10. Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.
11. Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.
12. V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.
13. Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií verejnej správy:
   a) operačné systémy,
   b) virtualizačné prostredia,
   c) aplikačný softvér,
   d) pracovné stanice,
   e) sieťové zariadenia, vrátane bezpečnostných zariadení,
   f) databázové prostredia.

14. Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.
15. Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

G. Hodnotenie zraniteľností a bezpečnostné aktualizácie

Nastavenie automatickej aktualizácie operačného systému a aplikácií.

1. Dodávateľ zavedie pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.
2. Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.
3. Vykonávanie hodnotenie zraniteľností najmenej raz ročne.
4. Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných technológií verejnej správy.
5. Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií.
6. Jednotlivé prvky informačných technológií verejnej správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií verejnej správy.
7. Primárnymi zdrojmi na identifikáciu nových zraniteľností a bezpečnostných aktualizácií sú
   a) informácie zo systémov a automatizovaných technológií pre aktualizáciu,
   b) informačný servis výrobcov technológií,
   c) výstupy z bezpečnostných technológií,
   d) výsledky penetračných testov,
   e) oznámenia a varovania orgánov štátnej správy a autorít v oblasti kybernetickej bezpečnosti,
   f) webové stránky a portály spoločností zameraných na publikovanie zraniteľnosti.
8. Výnimky z implementácie bezpečnostných aktualizácií sa schvaľujú a evidujú manažérom kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý určuje bezpečnostné opatrenia na ochranu pred zneužitím zraniteľnosti, na elimináciu ktorej je bezpečnostná aktualizácia vydaná.
9. Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií.
10. Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií verejnej správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou.
11. Po implementácii aktualizácie sa aktualizuje prvok informačných technológií verejnej správy verifikovaný, najmä jeho správna funkcionalita.
12. Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov.
13. Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.

H. Ochrana proti škodlivému kódu

1. Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom.
2. V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.
3. Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na
   a) používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD,
   b) škodlivé emailové prílohy a odkazy,
   c) podozrivé a škodlivé webové stránky a odkazy,
   d) externú a internú sieťovú komunikáciu u Dodávateľa vrátane webových sídiel,
   e) prenos súborov z externých sietí.
4. Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.
5. Zavedenie ochrany informačných technológií verejnej správy pred škodlivým kódom najmenej v rozsahu
   a) kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,

b) detekcie prítomnosti škodlivého kódu na všetkých používaných informačných technológiách verejnej správy,
c) kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
d) detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu.
6. Zavedenie ochrany pred nevyžiadanou elektronickou poštou.
7. Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu.
8. Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov.
9. Vypracovanie postupov obnovy a odstránenia infiltrácie škodlivým kódom na efektívne zvládanie infiltrácie škodlivým kódom.

I. Sieťová a komunikačná bezpečnosť

1. Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu.
2. Na sieťových zariadeniach sa implementujú najmenej tieto bezpečnostné opatrenia:
   a) pravidelná aktualizácia firmvéru,
   b) zmena továrensky nastavených autentifikačných údajov,
   c) pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
   d) vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu.
3. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.
4. Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.
5. Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.
6. Správa počítačových sietí je riadená a kontrolovaná.
7. Pri prenose údajov prostredníctvom verejnej siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb.
8. Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment.
9. Sieťové služby, používatelia a jednotlivé prvky informačných technológií verejnej správy musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni.
10. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia.
11. Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu.
12. Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov.
13. Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami.
14. Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu.
15. Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii.
16. Vzdialený prístup do vnútornej siete Dodávateľa musí podliehať autentifikácii a autorizácii.
17. Dodávateľ implementuje technológiu detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete.
18. Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.
19. Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.

J. Akvizícia, vývoj a údržba informačných technológií verejnej správy

1. Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Pri vytváraní nových alebo úprave existujúcich informačných technológií verejnej správy sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť.
3. Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov.
4. Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou.
5. Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.
6. Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien.
7. Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne.
8. Súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.
9. Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre Prevádzkovateľa, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.

K. Zaznamenávanie udalostí a monitorovanie

Zaznamenávanie úspešných a neúspešných autentifikačných udalostí.

1. Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií verejnej správy.
2. Pre každý prvok informačných technológií verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované.
3. Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej tieto udalosti:
   a) úspešné a neúspešné autorizačné udalosti,
   b) úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
   c) úspešné a neúspešné prístupy k log súborom,
   d) úspešné a neúspešné prístupy k systémovým zdrojom,
   e) vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
   f) zmeny v prístupových oprávneniach,
   g) aktivácia a deaktivácia bezpečnostných mechanizmov,
   h) spustenie a zastavenie procesov,
   i) konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
   j) spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
   k) významné aktivity v sieťovej komunikácii,
   l) požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
   m) IP adresy pridelené prostredníctvom služby DHCP.
4. Jednotlivé záznamy v log súboroch obsahujú najmenej tieto informácie o každej zaznamenanej udalosti, ak sú k dispozícii:
   a) čas a dátum udalosti,
   b) identifikácia používateľa,

c) identifikácia zariadenia,
d) informácia týkajúca sa udalosti,
e) indikácia úspešnosti, alebo zlyhania operácie,
f) pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port.

5. Záznamy udalostí sa uchovávajú najmenej šesť mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.
6. Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií verejnej správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.
7. Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.
8. Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja.
9. Dodávateľ vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií verejnej správy.
10. Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
11. Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.
12. Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.
13. Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.
14. Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením.
15. Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

L. Fyzická bezpečnosť a bezpečnosť prostredia

1. Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.
2. Umiestnenie informačných technológií verejnej správy v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa.
3. Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami.
4. Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám.
5. Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj pravidlá
   a) údržby, uchovávania a evidencie technických komponentov informačných technológií verejnej správy a zariadení informačných technológií verejnej správy,
   b) používania zariadení informačných technológií verejnej správy na iné účely, než na aké sú pôvodne určené,
   c) používania zariadení informačných technológií verejnej správy mimo určených priestorov,
   d) vymazávania, vyraďovania a likvidovania zariadení informačných technológií verejnej správy a všetkých typov relevantných záloh,
   e) prenosu technických komponentov informačných technológií verejnej správy alebo zariadení informačných technológií verejnej správy mimo priestorov orgánu riadenia,
   f) narábania s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačných technológií verejnej správy tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.
6. Prvky informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie.
7. Podporná infraštruktúra informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora.
8. Pre informačné technológie verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií verejnej správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.

M. Riešenie kybernetických bezpečnostných incidentov

1. Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií verejnej správy, ktoré sú zistené pri ich používaní alebo správe.
2. Dodávateľ má na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov.
3. Interný riadiaci akt podľa písmena b) obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií verejnej správy, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií verejnej správy potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.
4. S interným riadiacim aktom, najmä povinnosťou ohlasovať kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámia všetci používatelia informačných technológií verejnej správy vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií verejnej správy.
5. Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách verejnej správy sa vytvára kontaktné miesto.
6. Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu.
7. Proces odborného posúdenia a analýzy oznámení realizuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti v spolupráci so správcami jednotlivých komponentov a s vlastníkom/gestorom informačných technológií verejnej správy alebo príslušnou jednotkou CSIRT/CERT.
8. Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov.
9. Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy.
10. Poznatky získané z procesu riešenia bezpečnostného incidentu, najmä z analýzy a spôsobu vyriešenia, sa premietajú do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov, ako aj na zlepšenie detekcie alebo spôsobu riešenia obdobných bezpečnostných incidentov.
11. Zamestnanci poverení riešením kybernetických bezpečnostných incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.
12. Dodávateľ má vytvorené plány na riešenie kybernetických bezpečnostných incidentov.

N. Kryptografické opatrenia

Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=181

1. Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.
2. Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä
   a) elektronických dokumentov,
   b) dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
   c) emailovej komunikácie prostredníctvom PGP alebo S/MIME,
   d) komunikačných kanálov na výmenu nešifrovaných dát,
   e) centrálnych úložísk,
   f) záloh.
3. Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje najmä
   a) princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
   b) definovanie požadovanej úrovne ochrany a štandardy šifrovania,
   c) roly a zodpovednosti jednotlivých subjektov pri používaní šifrovania,
   d) riadenie šifrovacích kľúčov.

4. Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie.
5. Dodávateľ pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.

O. Kontinuita prevádzky informačných technológií verejnej správy

1. Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú.
2. Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy.
3. Plán kontinuity prevádzky obsahuje najmä:
   a) roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
   b) možné vplyvy na prevádzku informačných technológií verejnej správy,
   c) časový rámec obnovy,
   d) identifikáciu zdrojov potrebných na obnovu prevádzky,
   e) identifikáciu zamestnancov potrebných na obnovu prevádzky,
   f) identifikáciu dát a systémov potrebných na obnovu prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
   g) identifikáciu priestorov potrebných na obnovu prevádzky,
   h) stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov),
   i) identifikáciu vybavenia potrebného na obnovu prevádzky (procesy obnovy alebo výmeny kľúčových zariadení, alternatívne zdroje, vzájomná pomoc),
   j) spotrebný materiál potrebný na obnovu prevádzky (procesy výmeny zásob a kľúčových dodávok, zabezpečenie núdzových súčastí),
   k) konkrétne havarijné procedúry slúžiace na obnovu prevádzky.
4. Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne.

P. Audit a kontrolné činnosti

1. Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa tejto Zmluvy.
2. Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy.
3. Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti.
4. Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad.
5. Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijmú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravia sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.

PRÍLOHA 3
Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa v zmysle Základného kontraktu

Prevádzkovateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	Email
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej bezpečnosti		
		Zodpovedná osoba na úseku ochrany osobných údajov		
		Technická podpora		

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou základnej služby	Telefónny kontakt	Email
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej bezpečnosti		
		Zodpovedná osoba na úseku ochrany osobných údajov		
		Technická podpora		

PRÍLOHA 4
Zoznam schválených Subdodávateľov

Obchodné meno	Sídlo	IČO	Rozsah činností v zmysle Základného kontraktu

PRÍLOHA 5
Špecifikácia spracúvania osobných údajov

Základný kontrakt
Základným kontraktom, ktorý upravuje predmet zmluvného vzťahu medzi Prevádzkovateľom a Dodávateľom je Zmluva o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania špecifikovaná v Preambule tejto Zmluvy.

Prevádzkovateľ
Prevádzkovateľom podľa čl. 4 ods. 7 Všeobecného nariadenia o ochrane údajov je Hlavné mesto Slovenskej republiky Bratislava, ktorý určuje prostriedky a účely spracúvania osobných údajov.

Sprostredkovateľ
Sprostredkovateľom podľa čl. 4 ods. 8 všeobecného nariadenia o ochrane údajov je Dodávateľ:
_____ , ktorý spracúva osobné údaje v mene Prevádzkovateľa pri výkone činností špecifikovaných v Základom kontrakte.

Účel spracovania
Osobné údaje budú spracúvané na účely plnenia služieb definovaných Základným kontraktom:
bezproblémová, časovo a administratívne efektívna úhrada parkovného zákazníkmi Prevádzkovateľa prostredníctvom Dodávateľom vytvorenej a prevádzkovanej aplikácie a kontrola týchto úhrad integráciou aplikácie do systému ParkSys

Kategória dotknutých osôb
Zákazníci Prevádzkovateľa

Kategória údajov a ich jednotlivé atribúty (typy)
Bežné osobné údaje: titul, meno, priezvisko, adresa trvalého alebo prechodného pobytu, EČ motorového vozidla, vzťah k motorovému vozidlu, vzťah k držiteľovi/používateľovi motorového vozidla, miesto podnikania, miesto výkonu práce, vlastníctvo k nehnuteľnosti, vzťah k majiteľovi nehnuteľnosti, transakčné údaje
Osobitná kategória osobných údajov: zdravotný stav (ZŤP)

Prevádzkovateľom povolené operácie s osobnými údajmi
Dodávateľ spracúva osobné údaje automatizovanými prostriedkami, pričom ich môže získavať, zaznamenávať, usporadúvať, uchovávať, poskytovať Prevádzkovateľovi, prípadne schváleným Subdodávateľom prenosom, vymazávať alebo likvidovať len za podmienok uvedených v Základom kontrakte a v tejto Zmluve.

Doba spracúvania osobných údajov
- odo dňa účinnosti tejto Zmluvy po dobu jej trvania v súlade s jej článkom X. ods. 1