Príloha č. 1 k Dohode o poskytnutí prístupu k informačným technológiám

Špecifikácia predmetu dohody

A. Vzdialený prístup do informačných technológií Poskytovateľa

A.1 Vzdialený prístup pre Správcu a/alebo tretiu stranu do IT Poskytovateľa sa vytvára za účelom prístupu k IS GSAA z dôvodu používania, správy, údržby, úprav, aktualizácie, rozvoja a/alebo integrácie IS GSAA pre zachovanie jeho prevádzkyschopnosti alebo implementácie novej funkcionality (ďalej len „činnosti súvisiace s IS GSAA“).

A.2 Vzdialený prístup pre zamestnancov Správcu a/alebo tretej strany do IT Poskytovateľa je možný na základe udelených prístupových práv a vytvorených prístupových účtov prostredníctvom prihlasovacieho mena a prihlasovacieho hesla.

A.3 Vytvorenie vzdialeného prístup pre zamestnancov Správcu a/alebo tretej strany do IT Poskytovateľa vytvorí oprávnený zamestnanec Poskytovateľa na základe schválenej a predloženej žiadosti podľa prílohy č. 2 tejto dohody (ďalej len „žiadosť“).

A.4 Na základe schválenej žiadosti Poskytovateľom podľa bodu A.3 tejto časti za predpokladu dodržania pokynov a bezpečnostných dokumentov Poskytovateľa Správcom alebo treťou stranou, sprístupní Poskytovateľ IT vo svojej správe a prevádzke pre činnosti súvisiace s IS GSAA a súčasne vytvorí pre zamestnanca Správcu alebo tretej strany uvedeného na žiadosti vzdialený prístup. Na vytvorenie vzdialeného prístupu do IT poskytovateľa je potrebná súčinnosť používateľa, ktorý bude usmernený pokynmi Poskytovateľa.

A.5 Poskytovateľ poskytuje vzdialený prístup do IT Poskytovateľa pre Správcu bez akýchkoľvek záruk a vyhradzuje si právo dočasne prerušiť poskytovanie vzdialeného prístupu v prípade podozrenia na jeho zneužitie alebo hrozbu. Takéto prerušenie poskytovania vzdialeného prístupu nemôže byť chápané ako porušenie tejto dohody a Správca si z tohto titulu nemôže nárokovať akúkoľvek náhradu škody.

A.6 Správca je povinný pred zriadením vzdialeného prístupu do IT Poskytovateľa a následne aspoň raz štvrťročne predložiť Poskytovateľovi vyhlásenie o zabezpečení každého technického prostriedku Správcu alebo tretej strany podľa prílohy č. 3 tejto dohody, z ktorého sa bude vzdialene pripájať do IT Poskytovateľa.

A.7 Správca alebo tretia strana smie na vzdialené pripojenie do IT Poskytovateľa používať iba schválené technické prostriedky uvedené v žiadosti.

A.8 Správca a/alebo tretia strana budú činnosti súvisiace s IS GSAA vykonávať primárne prostredníctvom vzdialeného prístupu, v nevyhnutných prípadoch osobne v mieste inštalácie IS GSAA v objekte Poskytovateľa.

A.9 Správca alebo tretia strana je oprávnená využívať vzdialený prístup do IT Poskytovateľa pre činnosti súvisiace s IS GSAA počas pracovných dní v čase od 6:00 hod. do 18:00 hod. Ak Správca alebo tretia strana potrebujú pristupovať do IT Poskytovateľa v inom čase ako je uvedené v prvej vete, je potrebný súhlas oprávneným zamestnancom Poskytovateľa podľa článku III bodu 3.6 písm. c) alebo d) tejto dohody.

A.10 Na základe skutočností na strane Správcu alebo tretej strany, majúcich vplyv na používanie prístupových účtov, Správca podľa svojich potrieb je povinný požiadať Poskytovateľa o zriadenie alebo zrušenie vzdialeného prístupu do IT Poskytovateľa a to na základe schválenej žiadosti (napr. skončenie pracovno-právneho vzťahu, odchod na materskú dovolenku, zmena pracovného miesta a pod.).

A.11 V prípade podozrenia na odcudzenie alebo zneužitie používateľského hesla, BI alebo inú hrozbu Správca alebo tretia strana okamžite, po zistení takejto situácie, oznámi túto skutočnosť Poskytovateľovi elektronicky na elektronickú adresu v súlade s prílohou č. 1 časť D bod 1.1 tejto dohody. Následne Poskytovateľ dočasne zablokuje vzdialený prístup do IT Poskytovateľa zamestnancom Správcu alebo tretej strany do času vyriešenia nahlásenej situácie. Hlásenie musí obsahovať minimálne:

a) popis situácie,
b) meno a priezvisko zamestnanca Správcu alebo tretej strany, ktorému má byť dočasne zablokovaný vzdialený prístup do IT Poskytovateľa,
c) meno a priezvisko zamestnanca Správcu alebo tretej strany, ktorý situáciu identifikoval,

d) meno a priezvisko zamestnanca Správcu, ktorý situáciu nahlasuje.

V mimoriadnych prípadoch môže takéto hlásenie vykonať aj osoba, neuvedená na komunikáciu podľa článku III tejto dohody.

A.12 Správca je povinný pre evidenčné účely viesť zoznam vytvorených a zrušených prístupov do IT Poskytovateľa na základe tejto dohody.

B. Pohyb zamestnancov Správcu a tretej strany v objekte Poskytovateľa

B.1 Do objektu Poskytovateľa môžu vopred nahlásení zamestnanci Správcu a tretej strany vstupovať a z neho odchádzať len k tomu určenými vchodmi a východmi.

B.2 Zamestnanci Správcu a tretej strany sú povinní pri vstupe do objektu Poskytovateľa preukázať svoju totožnosť bezpečnostnej službe.

B.3 Zamestnanci Správcu a tretej strany sa môžu v objekte Poskytovateľa pohybovať len v sprievode určeného zamestnanca Poskytovateľa.

B.4 Zamestnanci Správcu a tretej strany sú povinní umiestniť si na viditeľnom mieste na vrchnej časti odevu návštevnú kartu, ak ju dostanú od bezpečnostnej služby, a pri odchode sú povinnú ju vrátiť bezpečnostnej službe.

B.5 Zamestnanci Správcu a tretej strany môžu vstupovať do zabezpečeného priestoru Poskytovateľa len v sprievode oprávneného zamestnanca Poskytovateľa.

B.6 V zabezpečených priestoroch Poskytovateľa je zakázané konzumovať jedlá a nápoje, narábať s kvapalinami, horľavými látkami a vykonávať také činnosti, ktorých dôsledkom by mohla byť spôsobená ekonomická škoda Poskytovateľovi.

B.7 Vynášanie údajov, zariadení alebo dokumentov patriacich Poskytovateľovi z objektov Poskytovateľa súvisiacich s činnosťami pre IS GSAA, je možné len s písomným súhlasom zodpovedného zamestnanca Poskytovateľa podľa prílohy č. 5 tejto dohody.

B.8 Správca, a tretia strana v súčinnosti s Poskytovateľom je povinná zabezpečiť poučenie svojich zamestnancov o všeobecne záväzných právnych predpisoch z oblasti bezpečnosti a ochrany zdravia pri práci a rovnako sú povinní počas trvania tejto dohody dodržiavať technické a bezpečnostné predpisy a riadiť sa primerane pokynmi Poskytovateľa.

B.9 V prípade, ak v priestoroch Poskytovateľa dôjde k pracovnému úrazu zamestnanca Správcu alebo tretej strany z dôvodu porušenia všeobecne záväzných právnych predpisov SR z oblasti bezpečnosti a ochrany zdravia pri práci technických alebo bezpečnostných predpisov Poskytovateľa zodpovednosť Poskytovateľa sa spravuje platnými všeobecne záväznými právnymi predpismi SR.

B.10 Zamestnanci tretej strany môžu do objektu Poskytovateľa vstupovať len v sprievode oprávneného zamestnanca Správcu podľa článku III bod 3.7 tejto dohody.

C. Bezpečnostné opatrenia pri vzdialenom prístupe do informačných technológií Poskytovateľa

C.1 Zamestnanec správcu a zamestnanec tretej strany je povinný pri vykonávaní činností v IT Poskytovateľa:

a) zachovávať mlčanlivosti všetkých o údajoch Poskytovateľa, s ktorými prišli do styku pri prístupe do IT Poskytovateľa, a to aj po ukončení tejto dohody, pracovného, resp. služobného pomeru,
b) rešpektovať operatívne pokyny Poskytovateľa,
c) všetky činnosti v IT Poskytovateľa vykonávať v súlade so všeobecne záväznými právnymi predpismi SR uvedenými v časti „Vymedzenie základných pojmov, zoznam skratiek a všeobecne záväzných právnych predpisov“ tejto dohody a vrátane príslušných vyhlášok k uvedeným všeobecne záväzným právnym predpisom,
d) prihlasovať sa do IT Poskytovateľa pod svojim prihlasovacím menom a prihlasovacím heslom na prístup do IT Poskytovateľa, zdieľanie prihlasovacích účtov viacerými používateľmi je zakázané,
e) zmeniť pri prvom prihlásení do IT Poskytovateľa prvé heslo na prístup do IT Poskytovateľa, ktoré bolo zamestnancovi Správcu a/alebo tretej strany pridelené Poskytovateľom,
f) zabezpečiť dôvernosť a ochranu svojho prihlasovacieho mena a prihlasovacieho hesla, pričom zodpovedá za všetky udalosti, zásahy a transakcie, ktoré sa uskutočnili v IT Poskytovateľa s použitím jeho prihlasovacieho účtu do IT Poskytovateľa,

g) v prípade podozrenia na prezradenie hesla, resp. v prípade jeho samotného prezradenia, o danej skutočnosti okamžite informovať zodpovedného zamestnanca Poskytovateľa a nahlásiť udalosť ako BI,
h) počas vzdialeného prístupu neopustiť pripojený technický prostriedok do IT Poskytovateľa, nedovoliť iným osobám prístup k tomuto technickému prostriedku alebo sledovanie jeho aktívnej obrazovky,
i) po ukončení vykonávania činností v IT Poskytovateľa odhlásiť sa z VPN a tak znemožniť prístup k IT Poskytovateľa, ktorý by mohol byť zneužitý k neoprávnenému prístupu do IT Poskytovateľa,
j) vykonávať činnosti v IT Poskytovateľa tak, aby pri ňom nedošlo k poškodeniu alebo zničeniu IT Poskytovateľa alebo k neočakávanému prerušeniu prevádzky IT Poskytovateľa,
k) v IT Poskytovateľa pristupovať len k IS GSAA, ak nie je v konkrétnych prípadoch dohodnuté inak.

C.2 Pri práci s heslom sú zamestnanci Správcu a tretej strany povinní dodržiavať nasledovné zásady:
a) musí obsahovať minimálne ,
b) musí obsahovať malé písmeno abecedy, veľké písmeno abecedy a číslo povolené sú aj písmená s diakritikou,
c) musí obsahovať špeciálny znak - symboly ako napr.: $ € ? , . : ; - _ ! / | \ = + [({]) } @ & # * ! ^ ` a iné, ak sú povolené,
d) nemôže obsahovať dva rovnaké znaky v rade za sebou (napr. AA, aa, 11 a pod.),
e) nemôže obsahovať chronologický sled minimálne troch po sebe nasledujúcich čísel vzostupne ani zostupne (napr. 123, 432),
f) nemôže byť tvorené priamou postupnosťou minimálne troch po sebe nasledujúcich klávesov na klávesnici v ľubovoľnom smere,
g) nemôže obsahovať názov ani sídlo zamestnávateľa, meno, priezvisko, prezývku (nickname), rolu, pracovné miesto, funkciu, dátum narodenia, telefónne číslo ani adresu používateľa, tzn. žiadne údaje, ktoré priamo alebo nepriamo identifikujú používateľa technického prostriedku,
h) neodporúča sa, aby obsahovalo písmená „Z“ alebo „Y“, z dôvodu používania viacerých možností rozloženia kláves na klávesnici („QWERTY“ alebo „QWERTZ“),
i) nemalo by byť príliš dlhé a príliš komplikované,
j)

k)

C.3 Pripájanie technických prostriedkov Správcu a/alebo tretej strany do IT Poskytovateľa v mieste inštalácie IS GSAA v objekte Poskytovateľa:
a) technické prostriedky Správcu a/alebo tretej strany (najmä osobné počítače, pamäťové nosiče údajov, meracie zariadenia, mobilné telefóny, tablety, sondy a pod.) v súvislosti s vykonávaním činností súvisiacich s IS GSAA v IT Používateľa je možné pripojiť do IT Používateľa len na základe písomného súhlasu zodpovedného zamestnanca Poskytovateľa podľa prílohy č. 4 tejto dohody,
b) ak sa do IT Poskytovateľa bude pripájať technický prostriedok Správcu a/alebo tretej strany, ktorý nie je schválený, je potrebné aby Správca predložil údaje o technickom prostriedku v rozsahu podľa prílohy č. 3 tejto dohody Poskytovateľovi na jeho posúdenie a schválenie,
c) vykonáva oprávnený zamestnanec Poskytovateľa podľa článku VIII bodu 3.6 písm. c) alebo d) tejto dohody,
d) technický prostriedok Správcu a/alebo tretej strany sa pripája k IT Poskytovateľa len na nevyhnutne potrebný čas, na základe výsledkov antivírusovej kontroly, ktorá potvrdí bezpečnosť technického prostriedku,
e) počas doby pripojenia technického prostriedku Správcu a/alebo tretej strany k IT Poskytovateľa v mieste inštalácie IS GSAA je prítomný určený zamestnanec Poskytovateľa.

C.4 Zamestnanci Správcu a tretej strany majú zakázané:
a) používať vzdialený prístup do IT Poskytovateľa na iný účel, ako bol uvedený v žiadosti,
b) poskytovať, sprístupňovať alebo zdieľať prístupové údaje do IT Poskytovateľa,

c) ukladať prístupové údaje do IT Poskytovateľa na ľahko dostupné média a miesta (papier, diár, nezabezpečený počítačový súbor/program, stôl, monitor a pod.),
d) vzdialene sa prihlasovať do IT Poskytovateľa sa v iných časoch ako na to určených, okrem vopred dohodnutých a schválených konkrétnych prípadov,
e) nechávať vzdialene prihlásený technický prostriedok do IT Poskytovateľa bez dozoru,
f) ostávať vzdialene prihlásený do IT Poskytovateľa počas inej vykonávanej činnosti, ako činnosti súvisiacej s IS GSAA,
g) pristupovať k iným častiam alebo komponentom IT Poskytovateľa, ktoré nie sú predmetom tejto dohody,
h) inštalovať v IT Poskytovateľa akýkoľvek počítačový program alebo technický prostriedok,
i) na bežné činnosti v IT Poskytovateľa súvisiace s IS GSAA používať privilegované prístupové oprávnenia vzhľadom na používateľskú rolu,
j) vzdialene sa prihlasovať do IT poskytovateľa technickými prostriedkami, ktoré neboli Poskytovateľom schválené v súlade s touto dohodou,
k) poskytovať údaje, ktoré získali alebo s ktorými prišli do styku počas vzdialeného prístupu do IT Poskytovateľa tretím osobám.

C.5 Správca a tretia strana zodpovedá za dôvernosť a ochranu svojich hesiel a zodpovedá za všetky udalosti a transakcie, ktoré sa uskutočnili v IT poskytovateľa s použitím prihlasovacieho účtu zamestnanca Správcu alebo zamestnanca tretej strany.

C.6 Ak Poskytovateľ zistí, že zamestnanci Správcu alebo tretej strany mali pokus o prístup k iným častiam alebo komponentom IT Poskytovateľa okrem IS GSAA alebo jeho komponentov, bude okamžite Správcovi a tretej strane zablokovaný vzdialený prístup do IT Poskytovateľa zo strany Poskytovateľa.

C.7 Zamestnanec Správcu alebo tretej strany bude automaticky odhlásený zo vzdialeného prístupu do IT Poskytovateľa po identifikovaní nečinnosti v IT Poskytovateľa .

C.8 Poskytovateľ má právo na okamžité blokovanie vzdialených prístupov do IT Poskytovateľa v prípade:
a) pri zistení BI alebo podozrení na BI ako aj o iných zistených skutočnostiach majúcich vplyv na zabezpečovanie informačnej a kybernetickej bezpečnosti prevádzkovaných IT Poskytovateľa,
b) pri podozrení na pristupovanie do iných častí IT Poskytovateľa ako IS GSAA,
c) pri podozrení na pristupovanie do IT Poskytovateľa neschváleným technickým prostriedkom.

C.9 Správca je povinný pravidelne minimálne každé 3 mesiace preskúmavať udelené prístupy do IS GSAA, ktoré majú súčasne udelený vzdialený prístup do IT Poskytovateľa a na základe výsledkov preskúmania požiadať o zrušenie vzdialeného prístupu do IT Poskytovateľa.

C.10 Správca a tretia strana sú povinní dodržiavať bezpečnostnú dokumentáciu Poskytovateľa, ktorú im Poskytovateľ sprístupnil na naštudovanie pred podpisom tejto dohody.

C.11 Správca a tretia strana sú povinní prijímať primerané bezpečnostné opatrenia pri vzdialenom prístupe do IT Poskytovateľa minimálne v rozsahu ako má stanovené Poskytovateľ podľa bodu C.10 tejto časti alebo sú definované v tejto dohode.

C.12 V objekte Poskytovateľa vykonáva tretia strana činnosti súvisiace s IS GSAA vždy pod dozorom oprávneného zamestnanca Správcu v súlade s článkom III bodom 3.7 písm. g) tejto dohody.

C.13 Správca prehlasuje, že súhlasí s bezpečnostnými opatreniami podľa tejto dohody a zaväzuje sa ich dodržiavať.

C.14 Správca zabezpečí do 10 pracovných dní po podpise tejto dohody súhlas s bezpečnostnými opatreniami podľa tejto dohody a záväzok dodržiavať ich od tretej stany.

D. Riadenie bezpečnostných udalostí

D.1 Zamestnanci Správcu a/alebo tretej strany vykonávajúci činnosti v IT Poskytovateľa sú povinní pri zistení bezpečnostnej udalosti majúcej vplyv na zabezpečovanie informačnej a kybernetickej bezpečnosti prevádzkovaných IT Poskytovateľa bezodkladne nahlásiť túto skutočnosť na určené kontaktné miesto, a to na elektronickú adresu Poskytovateľa .

D.2 Predmetom tejto dohody nie je riešenie bezpečnostných udalostí a bezpečnostných incidentov týkajúcich sa činnosti súvisiacich s IS GSAA.

D.3 Bezpečnostná udalosť musí byť konkrétne, nezameniteľne a zrozumiteľne špecifikovaná. Hlásenie vykonáva oprávnený zamestnanec Správcu podľa článku III bodu 3.7 tejto dohody.

D.4 Hlásenie o bezpečnostnej udalosti podľa bodu D.1 tohto článku obsahuje minimálne:

a) kontaktné údaje zamestnanca Správcu a/alebo tretej strany, ktorý identifikoval bezpečnostnú udalosť(názov Správcu alebo tretej strany, meno a priezvisko, elektronická adresa, telefónne číslo, lokalita - adresa, poschodie, miestnosť),
b) časové údaje zistenia a/alebo vzniku bezpečnostnej udalosti,
c) popis vykonávaných činností v IT Poskytovateľa pri identifikovaní bezpečnostnej udalosti,
d) detailný opis priebehu bezpečnostnej udalosti a jeho prvotnú identifikáciu alebo podozrenie (prejavy, správanie sa IT Poskytovateľa, ktoré naznačili/jednoznačne identifikovali bezpečnostnú udalosť),
e) zoznam zasiahnutých alebo potencionálne zasiahnutých častí/komponentov/aktív IT Poskytovateľa alebo IS GSAA BI (hostname, MAC adresu, IP adresu, identifikačné údaje zariadení, identifikácia IS a pod.), zoznam zasiahnutých alebo potencionálne zasiahnutých údajov, zoznam zúčastnených osôb, dátum a čas manipulácie s údajmi, vymedzenie miesta ich uloženia,
f) informáciu o vykonaných opatreniach smerujúcich k zmierneniu dopadov bezpečnostnej udalosti, vrátane dátumu a času realizácie opatrení.

D.5 Zamestnanci Správcu alebo tretej strany vykonávajúci činnosti v IT Poskytovateľa prostredníctvom vzdialeného prístupu sú povinní pri vyšetrovaní bezpečnostnej udalosti, ktorá súvisí s plnením tejto dohody, zamestnancom Poskytovateľa alebo iným príslušným orgánom, poskytnúť potrebnú súčinnosť.

D.6 Po vzniku bezpečnostnej udalosti nesmú zamestnanci Správcu a/alebo tretej strany vykonávajúci činnosti v IT Poskytovateľa prostredníctvom vzdialeného prístupu vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov bezpečnostnej udalosti.

D.7 Poskytovateľ rieši nahlásenú bezpečnostnú udalosť v rámci svojich kapacít v súlade so zákonom č. 69/2018 Z. z. a zákonom č. 95/2019 Z. z. a príslušných vyhlášok k uvedenému zákonu.

D.8 Poskytovateľ je povinný vyhodnotiť bezpečnostnú udalosť a prípadne ju označiť ako bezpečnostný incident (ďalej len „BI“). Za dočasné vyriešenie BI sa považuje i náhradný spôsob vyriešenia BI s cieľom zabezpečiť prevádzkyschopnosť IS GSAA, a to až do doby definitívneho vyriešenia BI alebo odstránenia dôsledkov BI.

D.9 Ak zistený BI bude mať za následok narušenie integrity, dostupnosti a dôvernosti služieb poskytovaných IS GSAA, všetky povinnosti vyplývajúce prevádzkovateľovi základnej služby zo zákona č. 69/2018 Z. z. a/alebo 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 znáša Správca.

D.10 Poskytovateľ eviduje všetky bezpečnostné udalosti a BI súvisiace so vzdialeným prístupom do IT Poskytovateľa identifikovaného pri vykonávaní činností súvisiacich s IS GSAA, ich prešetrenie, riešenie a uzatvorenie a aj prípadné nápravné opatrenia.

D.11 Poskytovateľ informuje Správcu o vyriešení bezpečnostné udalosti a/alebo BI súvisiaceho so vzdialeným prístupom do IT Poskytovateľa pre činnosti súvisiace s IS GSAA.

D.12 Správca je povinný v súvislosti so vzdialeným prístupom do IT Poskytovateľa na základe pokynov Poskytovateľa prijať nápravné opatrenia, ktoré boli schválené Poskytovateľom pri riešení bezpečnostnej udalosti a/alebo BI a súvisia s plnením predmetu tejto dohody.

E. Prevádzka IS GSAA

E.1 Poskytovateľ sa zaväzuje poskytnúť Správcovi pre činnosti súvisiace s IS GSAA technické a programové prostriedky a siete Poskytovateľa do času premiestnenia a inštalácie IS GSAA na technické a programové prostriedky Správcu v rozsahu:

a)
b)
c)
d)
e)
f)
g)
h

i)
j)
i)
j)

E.2 Poskytovateľ bude pre činnosti súvisiace s IS GSAA zabezpečovať:

a) nepretržité napájanie elektrickým prúdom technických prostriedkov, na ktorých je IS GSAA nainštalovaný,
b) dohľad a súčinnosť nad dostupnosťou vzdialeného prístupu do IT Poskytovateľa v režime 8/5, t. j. v pracovných dňoch v čase od 7:30 hod. do 15:30 hod.,
c) aktualizáciu OS,
d) aktualizáciu databázy údajov IS GSAA,
e) monitoring infraštruktúry,
f) úpravu sieťových nastavení,
g) manažment virtuálnej infraštruktúry,
h) manažment active directory (ďalej len „AD“),
i) manažment používateľských prístupov pre VPN,
j) poskytovanie mailových služieb – notifikácie a pod.,
k)

l)

m) služby siete internet,
n) umožniť Správcovi monitoring testovacieho a produkčného prostredia IS GSAA,
o) udržiavať integračné rozhranie na externé informačné systémy, s ktorými sa IS GSAA integruje (napr. IACS),
p) zaznamenávanie udalostí a monitorovanie súvisiace s prihlasovaním do IT poskytovateľa a na požiadanie Správcu mu tieto sprístupní,
o) iné podľa vzájomnej dohody Strán dohody.

E.3 Plánovanú nedostupnosť vzdialeného prístupu do IT Poskytovateľa pre činnosti súvisiace s IS GSAA Poskytovateľ oznámi Správcovi minimálne 3 pracovné dni vopred. Poskytovateľ sa zaväzuje, že plánovanú údržbu IT bude vykonávať prioritne v pracovných dňoch medzi hod. až hod. a podľa vzájomnej dohody Strán dohody.

E.4 Správca bude nahlasovať nedostupnosť vzdialeného prístupu do IT Poskytovateľa pre činnosti súvisiace s IS GSAA podľa článku III bodu 3.7 písm. c) a d) tejto dohody.

E.5 Poskytovateľ poskytne súčinnosť pri premiestnení IS GSAA na technické a programové prostriedky Správcu.

E.6 Na účel premiestnenia a inštalácie IS GSAA na technické a programové prostriedky Správcu bude zriadená pracovná skupina zložená z určených zamestnancov Poskytovateľa, Správcu a tretej strany. Zo stretnutí pracovnej skupiny sa budú vyhotovovať písomné zápisnice. Účelom zriadenia pracovnej skupiny bude najmä organizačné a technické zabezpečenie premiestnenia a inštalácie IS GSAA na technické a programové prostriedky Správcu.

E.7 Pri ukončení tejto Dohody (po premiestnení a nainštalovaní IS GSAA na technické a programové prostriedky Správcu) bude vypracovaný preberací a odovzdávací protokol podľa prílohy č. 6 tejto dohody, kde bude preukázateľne potvrdené odovzdanie IS GSAA do výhradnej a úplnej správy a prevádzky Správcovi.