Zmluva o poskytnutí služieb

Uzavretá v zmysle § 269 ods. 2 zák. č. 513/1991 Zb. Obchodný zákonník
v znení neskorších predpisov

1. OBJEDNÁVATEĽ:

Názov:	**Finančné riaditeľstvo Slovenskej republiky**
Zastúpené:	Ing. František Imrecze, prezident finančnej správy
Sídlo:	Lazovná 63, 974 01 Banská Bystrica
IČO:	42499500
	(ďalej len „objednávateľ")

2. POSKYTOVATEĽ:

Názov:	**DataCentrum - CSIRT.SK**
Zastúpené:	Ing. Mojmír Kollár, riaditeľ DataCentra
Sídlo:	Cintorínska 5, 814 88 Bratislava
IČO:	00151564
	(ďalej len „poskytovateľ")

Čl. I.
Predmet zmluvy

1. Na základe tejto Zmluvy sa poskytovateľ zaväzuje vykonať pre objednávateľa interné a externé penetračné testovanie bližšie popísané v Prílohe č.1 tejto Zmluvy.
2. Penetračným testovaním (ďalej len „testovanie") je konanie súvisiace s prienikom do počítačového systému.
3. Poskytovateľ sa zaväzuje na záver testovania najneskôr do 31.12.2015 vypracovať pre objednávateľa záverečnú správu, ktorá bude obsahovať výsledok testovania a navrhnuté opatrenia.
4. V prípade, že bude pri testovaní zistený taký typ zraniteľnosti, za pomoci ktorej bude možné preniknúť do systému objednávateľa a získať nad ním kontrolu s pravdepodobnou možnosťou poškodenia systému, poskytovateľ je povinný zastaviť činnosť, zdokumentovať tento stav, oboznámiť objednávateľa s touto skutočnosťou a navrhnúť možné riešenie.
5. Objednávateľ berie na vedomie, že predmetom tejto Zmluvy je reálny tzv. hackerský útok za použitia invazívnych techník, ktorý môže reálne ohroziť fungovanie a prevádzku nie len testovaných systémov, ale aj iných súvisiacich systémov Objednávateľa a ďalších štátnych orgánov.

Čl. II.
Termín a miesto plnenia

1. a) Miestom plnenia externej časti penetračného testu je DataCentrum, Cintorínska 5, 814 88 Bratislava a
   b) miestom plnenia internej časti penetračného testu je Finančná správa, Mierová 23, 815 11 Bratislava.
2. Termín plnenia Zmluvy začína plynúť dňom nadobudnutia jej účinnosti.
3. Zmluva sa uzatvára na dobu určitú s platnosťou do 31.12.2015.

Čl. III.
Odškodnenie a zodpovednosť

Objednávateľ prehlasuje, že bol v zmysle čl. I. odsek 5 tejto Zmluvy upozornený poskytovateľom na možné riziká súvisiace s testovaním.

Čl. IV.
Ochrana informácií

1. Objednávateľ týmto poučuje poskytovateľa o skutočnosti, že informácie ktoré sa dozvie pri plnení tejto dohody, môžu byť predmetom daňového tajomstva. O tejto skutočnosti je poskytovateľ povinný poučiť aj svojich zamestnancov a osoby, ktoré budú v jeho mene plniť túto dohodu.
2. Poskytovateľ podpisom tejto dohody prehlasuje, že bol poučený o povinnosti zachovať daňové tajomstvo podľa § 11 zákona č. 563/2009 Z.z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a o právnych dôsledkoch porušenia tejto povinnosti.
3. Poskytovateľ sa zaväzuje dodržiavať Všeobecné podmienky o zabezpečení informačnej bezpečnosti finančnej správy v súvislosti s prístupom k informačno-komunikačným technológiám finančnej správy, s výnimkou ustanovení písm. f), g), l), m) a j) v časti „neočakávané prerušenie prevádzky" odst. 2 článku 2 Základných požiadaviek.
   Všeobecné podmienky o zabezpečení informačnej bezpečnosti finančnej správy tvoria Prílohu č. 2 tejto Zmluvy.
4. Zmluvné strany sú povinné zachovávať mlčanlivosť o skutočnostiach týkajúcich sa vykonania testovania. Ďalej sú zmluvné strany povinné zachovávať mlčanlivosť o akýchkoľvek informáciách, o ktorých sa dozvedeli pri uzatváraní tejto zmluvy alebo počas jej trvania pri výkone svojich práv a povinností z nej vyplývajúcich, najmä ich nesmú prezradiť tretej osobe, ani ich použiť v rozpore s účelom ich poskytnutia, to sa nevzťahuje na použitie výsledkov testovania objednávateľom na účely rozvoja a zvýšenia úrovne bezpečnosti informačných technológii a definovania nápravných opatrení.

Čl. V.
Odmena

Zmluvné strany sa dohodli, že poskytovateľ poskytne testovanie, uvedené v čl. I zmluvy, pre objednávateľa bezodplatne.

Čl. VI.
Záverečné ustanovenia

1. Zmluva nadobúda platnosť a účinnosť dňom jej podpísania oprávnenými zástupcami oboch strán.
2. Zmluvné strany vynaložia všetko úsilie na zmierne vyriešenie všetkých nezhôd alebo sporov vznikajúcich medzi nimi pri plnení zmluvy alebo v súvislosti s ňou, a to cestou priamych rokovaní.
3. Táto zmluva je vyhotovená v štyroch rovnopisoch, z ktorých dva obdrží objednávateľ a dva poskytovateľ.
4. Zmluvné strany osvedčujú, že zmluvu uzavreli slobodne, vážne, bez nátlaku, bez omylu, túto si pred jej podpisom prečítali, jej obsahu porozumeli a na znak súhlasu s jej obsahom ju podpísali.

Za objednávateľa:

V Bratislave, dň[redacted]

[redacted]

Ing. František Imrecze

Za poskytovateľa:

V Bratislave, dňa[redacted]

[redacted]

Ing. Mojmír Kollár

DOTAZNÍK K INTERNÉMU A EXTERNÉMU PENETRAČNÉMU TESTOVANIU

1. Kontakt (uveďte, akým spôsobom a kedy je možné kontaktovať uvedenú osobu v prípade potreby resp. stavu núdze):

PFS
[redacted]
metodik
Finančné riaditeľstvo SR
[redacted]@financnasprava.sk
048/4393382
0905334668

ISFS SD
[redacted]
metodik
Finančné riaditeľstvo SR
[redacted]@financnasprava.sk
048/4393552
0903721485

ISFS SD
[redacted]
metodik
Finančné riaditeľstvo SR
[redacted]@financnasprava.sk
048/4393502
0903550112

Sieťová infraštruktúra
[redacted]
metodik
Finančné riaditeľstvo SR
[redacted]@financnasprava.sk
02/40202914
0903401788

Bezpečnosť
[redacted]
špecialista pre IT bezpečnosť a licenčnú politiku
Finančné riaditeľstvo SR
[redacted]@financnasprava.sk
047/4315216
0915398201

2. IP adresa/adresy (poskytovateľ), z ktorých bude prebiehať externé testovanie: *85.248.149.41 – 85.248.149.46, 85.248.149.53, 85.248.149.56, 85.248.149.57, 92.245.216.205.*

3. IP adresa/adresy (objednávateľ), ktoré budú predmetom externého testovania: 194.1.0.29, 10.100.201.250, 10.100.201.41, 10.100.201.26, 10.100.201.35, 10.100.201.36, 10.100.201.20, 10.100.201.21

4. Ciele vulnerability scanu identifikovanie zraniteľností a popis rizika spojeného s týmito zraniteľnosťami, uvedenie návrhov/odporúčaní na ich odstránenie

5. Časovanie testov (čas od - do, kedy by mali testy prebiehať):
   externé: 24 x 7
   interné: 24 x 7

6. Iné dôležité informácie:

---

7. Kontaktná osoba poskytovateľa:
   Meno: [redacted]
   Funkcia: vedúci oddelenia NIKI
   Email: [redacted]*@csirt.gov.sk*
   Telefónne číslo/mobil: +421 917 699 002
   Čas kedy je možné volať: 24/7

   Meno: [redacted]
   Funkcia: systémový inžinier II
   Email: [redacted]*@csirt.gov.sk*
   Telefónne číslo/mobil: +421 905 939 122
   Čas kedy je možné volať: 24/7

Príloha č.2

Všeobecné podmienky o zabezpečení informačnej bezpečnosti finančnej správy SR*

1. Úvodné ustanovenia

Tieto *Všeobecné podmienky,* pre zabezpečenie informačnej bezpečnosti finančnej správy SR (ďalej len *„všeobecné podmienky, resp. dohoda"*) stanovujú povinnosti tretej strany, ak predmet plnenia zmluvy uzatvorenej medzi treťou stranou a Finančným riaditeľstvom (ďalej len „FR") SR alebo Ministerstvom financií (ďalej len „MF") SR (ďalej len „zmluva") súvisí s informačno-komunikačnými technológiami Finančnej správy SR (ďalej len „IKT FS SR").

2. Výklad a definícia pojmov

1. Na účely tohto dokumentu

   a) **aktívum** je všetko, čo má pre Finančnú správu (ďalej len „FS SR") hodnotu (fyzické komponenty, softvér, dáta, služby, ľudské zdroje, povesť FS SR, ...),

   b) **bezpečnostným incidentom** je akýkoľvek spôsob narušenia bezpečnosti IKT, ako aj akékoľvek porušenie bezpečnostnej politiky a súvisiacich pravidiel,

   c) **DataCentrom** je samostatná rozpočtová organizácia so sídlom v Bratislave, ktorej zriaďovateľom je Ministerstvo financií SR. DataCentrum zabezpečuje vzájomnú prepojiteľnosť častí informačného systému rezortu MF SR a bezpečnosť informačného systému rezortu MF SR,

   d) **dostupnosť** je vlastnosť, že autorizovaní užívatelia majú v prípade požiadavky prístup k informáciám a aktívam,

   e) **dôvernosť** je vlastnosť, že informácia nie je dostupná alebo prístupná neautorizovaným jednotlivcom, entitám alebo procesom,

   f) **externý prístup** je prístup tretích strán ako i interných zamestnancov FS SR,

   g) **externým subjektom** je právnická osoba a štatutárom právnickej osoby určené fyzické osoby (ďalej len „zamestnanci externého subjektu"), ktoré nie sú zamestnancami FS a ktoré poskytujú FS služby v zmysle platných zmlúv, podľa ktorých môžu požiadať o prístup k IKT v presne určenom nevyhnutnom rozsahu,

   h) **externým prístupom zamestnanca FS k IKT** je iný prístup zamestnanca FS k IKT ako prístup zo štandardného pracoviska FS s LAN/WAN prepojením,

   i) **externým prístupom zamestnancov externého subjektu k IKT** je prístup zamestnanca externého subjektu k IKT,

   j) **FR SR** je Finančné riaditeľstvo SR,

   k) **FS SR** je Finančná správa SR,

   l) **IKT** sú informačno-komunikačné technológie,

---

* V prípade zmluvy uzatvorenie medzi treťou stranou a FR SR pôjde o Všeobecné podmienky o zabezpečení informačnej bezpečnosti Finančných orgánov SR a v prípade zmluvy medzi treťou stranou a MF SR pôjde o Dohodu o zabezpečení informačnej bezpečnosti Finančných orgánov SR.

m) **IKT FS SR** je súhrn nasledovných komponentov používaných na prípravu a spracovanie dát a na manažovanie informácií a procesov vo FS SR, okrem tých, ktoré sú verejne prístupné z vonkajšieho prostredia FS SR (napr. finančný portál):

1. servery, pracovné stanice, faxy a príslušná dokumentácia,
2. informačné systémy FS (aplikačné programové vybavenie a jeho vrstvy, ako napr. aplikačné servery, databázové servery) a príslušná dokumentácia,
3. dáta a informácie spracovávané v informačných systémoch FS,
4. zariadenia diskových polí, SAN infraštruktúra, zálohovacie zariadenia a príslušná dokumentácia,
5. sieťová infraštruktúra a sieťové komponenty (napr. smerovače, firewally) a príslušná dokumentácia,
6. zariadenia pre hlasovú komunikáciu implementované v sieťovej infraštruktúre FS (napr. pobočkové ústredne) a príslušná dokumentácia,
7. písomné záznamy súvisiace s IS FS SR.

n) **IP adresa** je adresa zariadenia pripojeného do počítačovej siete, definovaná na základe Internet Protokolu,

o) **informačné aktívum** je aktívum v prostredí IKT FS SR,

p) **informačná bezpečnosť** je súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných aktív,

q) **informačný systém** je súbor činností, ktoré zabezpečujú zber, prenos, spracovanie, uloženie, výber, distribúciu a prezentáciu informácií a dát (vrátane dát v papierovej podobe) pre potreby rozhodovania tak, aby riadiaci pracovníci mohli vykonávať funkcie riadenia vo všetkých zložkách systému riadenia,

r) **integrita** je vlastnosť, že informácie a metódy ich spracovania sú presné a kompletné,

s) **IS** je informačný systém,

t) **IS FS SR** je súhrn všetkých informačných systémov FS SR,

u) **kontaktná osoba** je SLA manažér tak za FS SR ako i za tretiu stranu,

v) **LAN/WAN** je štandardná lokálna počítačová sieť a prepojenie komunikačných sietí pracovísk FS realizované spravidla technológiou MPLS v rámci rezortnej komunikačnej siete a spravovanej DataCentrom,

w) **manažér bezpečnosti** je zamestnanec Oddelenia bezpečnosti Kancelárie prezidenta FR SR zodpovedný za celkovú bezpečnosť vo FS,

x) **manažér informačnej bezpečnosti IKT** je zamestnanec Oddelenia bezpečnosti Kancelárie prezidenta FR SR zodpovedný za bezpečnosť IKT vo FS,

y) **MF SR – Ministerstvo financií SR**

z) **organizačným útvarom** sú organizačné útvary FR SR,

aa) **oprávnená osoba** sú všetci zamestnanci sekcie informatiky FS SR, prípadne iný zamestnanec písomne poverený námestníkom sekcie informatiky na výkon úloh vyplývajúcich z činností spojených s tretími stranami a s externými prístupmi interných zamestnancov,

bb) **osobitná tretia strana** je NKÚ resp. iný kontrolný alebo oprávnený orgán SR podľa príslušného všeobecne záväzného právneho predpisu,

cc) **outsourcing** je zabezpečenie podporných služieb externou organizáciou,

dd) **používateľom externého prístupu je** zamestnanec FS alebo zamestnanec externého subjektu, ktorému bol povolený externý prístup k IKT,

ee) **prístup tretej strany k IKT FS SR** je prístup tretej strany k hardvéru alebo softvéru alebo dátam IKT FS SR vrátane príslušnej dokumentácie za nasledujúcich podmienok:

1. tretia strana má s FR SR podpísanú zmluvu o dodávaní alebo odoberaní tovarov, služieb alebo prác súvisiacich s IKT FS SR, ktorej súčasťou sú Všeobecné podmienky o zabezpečení informačnej bezpečnosti FS SR,
2. tretia strana má s MF SR podpísanú zmluvu o dodávaní alebo odoberaní tovarov, služieb alebo prác súvisiacich s IKT FS SR a s FR SR uzatvorenú Dohodu o zabezpečení informačnej bezpečnosti FS SR (ďalej len „dohoda"), ktorej obsahom budú vhodne upravené všeobecné podmienky vo forme dohody medzi FR SR a treťou stranou. Za takúto dohodu sa bude považovať aj dohoda uzatvorená s DR SR alebo s CR SR pred vznikom FR SR,
3. tretia strana realizuje dodávanie alebo odoberanie tovarov, služieb alebo práce súvisiace s IKT FS SR na základe outsourcingu, kde súčasťou tohto vzťahu sú Všeobecné podmienky o zabezpečení informačnej bezpečnosti FS SR,
4. tretia strana má od FR SR iba objednávku bez zmluvného vzťahu súvisiacu s hardvérom, softvérom, údržbou alebo službou súvisiacou s IKT FS SR,
5. treťou stranou je osobitná tretia strana.

ff) **Service Level Agreement (ďalej len „SLA")** je zmluva alebo dohoda medzi dodávateľom (externým alebo interným) a odberateľom služby IKT, ktorá dokumentuje dojednané parametre danej služby IKT,

gg) **SLA manažéri** sú zamestnanci FS zodpovední za riadenie úrovne poskytovaných služieb externým subjektom, alebo zamestnanci tretej strany zodpovední za prípravu, spracovanie a realizáciu konkrétnych požiadaviek externého prístupu k IKT FS SR. Obvykle sú to osoby z prostredia IKT,

hh) **tretie strany** sú externí dodávatelia a externí odberatelia vybraných služieb FR SR. V tejto súvislosti ide predovšetkým o externé subjekty, ktoré na zmluvnom základe s FR SR alebo MF SR dodávajú pre FR SR alebo odoberajú od FR SR špecializované údaje alebo vykonávajú pre FR SR špecializované práce súvisiace s návrhom, implementáciou, testovaním, dodávaním, údržbou, aktualizáciou alebo outsorucingom IKT, ako aj o ich subdodávateľov,

ii) **vedúci zamestnanec**

1. vedúci zamestnanec podľa § 9 zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov,
2. vedúci štátny zamestnanec podľa § 11 zákona č. 400/2009 Z. z., a
3. nadriadený podľa § 4 zákona č. 200/1998 Z. z.

jj) **VPN kanál** je bezpečnostný kanál, ktorý vytvára šifrované spojenie na pripojenie tretej strany k IKT FS SR na základe Virtual Private Network techník,

kk) **vzdialený prístup** je prístup tretej strany k softvéru alebo dátam IKT FS SR z iného miesta ako z priestorov FS SR.

ll) **zamestnancom FS**

1. zamestnanec vykonávajúci prácu vo verejnom záujme v zmysle zákona č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov,
2. zamestnanec v štátnozamestnaneckom pomere v zmysle zákona č. 400/2009 Z.z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 400/2009 Z. z."), a

3. colník, ktorý vykonáva štátnu službu podľa zákona č. 200/1998 Z. z. o štátnej službe colníkov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 200/1998 Z. z.").

mm) **zásah do IKT** sa rozumie akýkoľvek prístup do alebo k IKT, ktorý bol povolený tretej strane na základe žiadosti o povolenie prístupu.

2. Základné požiadavky

1. Tretia strana sa zaväzuje oboznámiť svojich zamestnancov zúčastňujúcich sa na predmete plnenia zmluvy s bezpečnostnými požiadavkami v rozsahu uvedenom v týchto všeobecných podmienkach pre zabezpečenie informačnej bezpečnosti FS SR.

2. Tretia strana sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov, realizujúcich predmet plnenia zmluvy, dodržiavanie týchto povinností:

   a) dodržiavať ochranu údajov a informácií súvisiacich s IKT a s existujúcimi alebo vyvíjanými informačnými systémami FS SR a záväzok mlčanlivosti o údajoch a informáciách, s ktorými počas výkonu prác vo FS SR prišli do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní, a to aj po ukončení pracovného, resp. zmluvného pomeru,

   b) zachovávať daňové tajomstvo, s ktorým počas výkonu prác vo FS SR prišli do styku, ako aj zákaz jeho využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a to aj po ukončení pracovného pomeru, resp. zmluvného pomeru,

   c) zachovávať mlčanlivosť o osobných údajoch, s ktorými počas výkonu prác vo FS SR prišli do styku, ako aj zákaz ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov pri plnení jeho úloh,

   d) preukázať na vyzvanie svoju totožnosť buď zamestnancom strážnej služby alebo oprávnenej osobe určenej na priamu komunikáciu s ním (ďalej iba oprávnená osoba) pri vstupe do priestorov FS SR, ak strážna služba nie je zriadená,

   e) realizovať zásahy do IKT FS SR iba v určenom rozsahu v rámci poskytovania dohodnutých prác a služieb pre FS SR,

   f) použiť len také externé pripojenia k IKT FS SR, ktoré sú uvedené v písomnej žiadosti o prístup externého subjektu k IKT FS SR,

   g) použiť externé pripojenia k IKT FS SR len spôsobom, ktorý nie je v rozpore so všeobecne záväznými právnymi predpismi a bezpečnostnými politikami FS SR,

   h) používať externé pripojenia k IKT FS SR výhradne na plnenie povinností v zmysle platnej zmluvy uzatvorenej s cieľom poskytnutia služieb externého subjektu v prospech FS SR,

   i) neposkytnúť svoju elektronickú identitu (napr. login, heslo, a pod.) inej osobe,

   j) realizovať výkon dohodnutých prác a služieb tak, aby pri nich nedošlo k poškodeniu alebo zničeniu kľúčových komponentov IKT alebo k neočakávanému prerušeniu ich prevádzky,

   k) riadiť sa pokynmi oprávnenej osoby, SLA manažéra FS SR, manažéra bezpečnosti a manažéra informačnej bezpečnosti IKT FS SR počas výkonu dohodnutých prác a služieb pre FS SR,

   l) zdokumentovať všetky zásahy do IKT FS SR podľa pokynov oprávnenej osoby a bezodkladne jej ohlásiť zistené bezpečnostné nedostatky, ktoré by mohli spôsobiť ohrozenie dôvernosti alebo integrity kódu alebo dokumentácie systému,

   m) pripájať svoje technologické prostriedky (napr. počítač, notebook, meracie prístroje a pod.) k IKT FS SR len po predchádzajúcom súhlase oprávnenej osoby, a to len na nevyhnutne

potrebnú dobu a s rešpektovaním podmienok spojených so súhlasom, ako napríklad antivírusová kontrola a podobne,

n) možnosti vynášať zariadenia, materiál a údaje patriace FS SR (informačno-komunikačné zariadenia, výsledky zostáv vytvorených na základe skriptov, zbery údajov, poskytované údaje, a pod.) z priestorov FS SR len s písomným súhlasom oprávnenej osoby, pričom zdokumentovaná e-mailová komunikácia je v odôvodnených a naliehavých prípadoch považovaná za súhlas oprávnenej osoby na priamu komunikáciu so žiadateľom,

o) rešpektovať autorské práva k materiálom poskytnutým z FS SR, na ktoré bola tretia strana upozornená,

p) vrátiť všetky materiály a údaje vrátane elektronických poskytnuté z FS SR a zlikvidovať všetky ich kópie, ak to nebolo zmluvne dohodnuté inak.

3. Doplňujúce požiadavky

1. V prípade, že predmet plnenia zmluvy súvisí s vývojom a aktualizáciou IKT FS SR, tretia strana akceptuje nasledujúce požiadavky:

   a) dodržiavanie bezpečnostných požiadaviek relevantných interných riadiacich aktov FS SR, bezpečnostných politík FS SR, platnej bezpečnostnej legislatívy (najmä požiadaviek zákona č.275/2006 Z.z. o informačných systémoch verejnej správy v znení neskorších predpisov a súvisiaceho výnosu), zachovávania mlčanlivosti o skutočnostiach zistených počas vývoja, nasadzovania a podpory vyvíjaného alebo aktualizovaného IS, zachovávanie mlčanlivosti týkajúcej sa daňového tajomstva a zachovávanie mlčanlivosti podľa § 18 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov

   b) nevnesenie nepožadovaného kódu a nepožadovaných funkcií do IS, ktoré by mohli viesť k zneužitiu IS neautorizovanými prístupmi a osobami,

   c) zabezpečenie ochrany dôvernosti a integrity kódu a dokumentácie systému (do kontaktu s kódom a dokumentáciou systému môžu prichádzať iba tí zamestnanci tretej strany, ktorí podpísali Poučenie zamestnancov externého subjektu o informačnej bezpečnosti v prostredí IKT FS SR (ďalej len „poučenie"),

   d) povinnosť vopred deklarovať, podľa akej vývojovej metodiky, resp. normy postupuje pri vývoji systému, pričom tento postup musí byť schválený FR SR,

   e) právo FS SR vykonať audit svojho vývojového prostredia. Účelom tohto auditu je súlad vývoja s deklarovanou metodikou, resp. normou,

   f) súhlas s poskytnutím potrebnej súčinnosti audítorovi vykonávajúcemu audit IS, ak tento IS súvisí s predmetom zmluvy. V prípade, ak potreba súčinnosti podľa tohto bodu na strane tretej strany presiahne rozsah 20 (dvadsať) človekohodín, tretia strana nie je povinná poskytnúť súčinnosť bez dohody o úhrade nákladov na takúto súčinnosť,

   g) súhlas s poskytnutím potrebnej súčinnosti FS SR pre prípadný audit svojich informačných systémov a IKT, ak tieto súvisia s predmetom plnenia zmluvy. V prípade, ak potreba súčinnosti podľa tohto bodu na strane tretej strany presiahne rozsah 20 (dvadsať) človekohodín, tretia strana nie je povinná poskytnúť súčinnosť bez dohody o úhrade nákladov na takúto súčinnosť,

   h) zabezpečenie, aby predmet plnenia zmluvy obsahoval aj bezpečnostné požiadavky pre vyvíjaný alebo aktualizovaný IS

   i) menovanie kontaktnej osoby* (SLA manažér) FS SR zodpovednej za informačnú bezpečnosť a činnosti podľa písmena a) až h) týchto doplňujúcich požiadaviek,

---

* Meno kontaktnej osoby za FS SR sa bude uvádzať v žiadosti o prístup externého subjektu k IKT FS SR

j) menovanie kontaktnej osoby** (SLA manažér) tretej strany zodpovednej za informačnú bezpečnosť a činnosti podľa písmena a) až h) týchto doplňujúcich požiadaviek,

k) vykonanie testovania pre činnosti súvisiace s bezpečnostnými požiadavkami súvisiacimi s vyvíjaným alebo aktualizovaným IS a vytvorenie dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch, a to najmenej vykonanie interného používateľského testovania v rozsahu minimálne jedného týždňa pred odovzdaním informačného systému, jeho časti alebo súvisiacej aplikácie a zahrnutie jeho výstupov do dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch,

l) dodanie dokumentácie pre nové alebo aktualizované IKT alebo ich časti, ktorá obsahuje:

1. používateľskú dokumentáciu, ktorou je návod na používanie systému, scenáre činností so systémom pre jednotlivé roly, pravidlá používania systému, opis bezpečnostných procedúr a ovládanie bezpečnostných mechanizmov, opis chybových hlásení,
2. prevádzkovú a administrátorskú dokumentáciu, ktorou je dokumentácia o architektúre informačného systému alebo jeho časti, popis prevádzkových postupov, postupy zotavenia sa z bežných chýb, rozdelenie rolí pri prevádzke a administrácii systému, opis konfigurácie systému a umiestnenia jednotlivých fyzických, aplikačných a dátových komponentov, väzby na existujúce informačné systémy, politiku použitia kryptografických opatrení, podrobný opis aktivít vyžadovaných pri administrácii systému, šablóny administrátorských a operátorských denníkov a uvedenie typov udalostí, ktoré sa do nich zapisujú.

m) nesplnenie bezpečnostných požiadaviek podľa písm. a) až l) s výnimkou písm. h) tohto odseku bude dôvodom na neukončenie príslušnej etapy projektu alebo neschválenie prevzatia vykonávanej činnosti.

2. V prípade, že predmet plnenia zmluvy sa priamo dotýka prístupu k IKT FS SR, tretia strana okrem požiadaviek uvedených v odseku 4 tohto článku akceptuje nasledujúce doplňujúce požiadavky:

a) zabezpečí realizovanie prístupu k softvéru alebo dátam IKT FS SR na základe žiadosti o prístup externého subjektu k IKT FS SR (ďalej len „žiadosť") podľa prílohy č. 2. V žiadosti musí byť uvedený dôvod prístupu, rozsah prístupu (časť IKT, resp. IS, ku ktorému je požadovaný prístup), miesto prístupu a IP adresa zariadenia na prístup (v prípade vzdialeného prístupu), stanovený dátum a čas prístupu a mená zamestnancov tretej strany, pre ktorých je požadovaný prístup. Záležitosti súvisiace so žiadosťou sa realizujú prostredníctvom kontaktných osôb a oprávnených zamestnancov. Žiadosť tretej strany o prístup k IKT FS SR podpísaná kontaktnou osobou za tretiu stranu, sa elektronicky (emailom so zoskenovanou žiadosťou alebo faxom), poštou alebo osobne doručí kontaktnej osobe FS SR. Kontaktná osoba FS SR doručí schválený resp. neschválený súhlas s prístupom k IKT FS SR elektronicky, poštou alebo osobne kontaktnej osobe tretej strany.

b) zabezpečí, aby všetci jej zamestnanci realizujúci prístup k IKT FS SR na základe pokynov kontaktnej osoby FS SR alebo oprávneného zamestnanca podpísali pred prvým prístupom k IKT FS SR poučenie podľa prílohy č. 3. V prípade odmietnutia podpísania tohto poučenia, nebude príslušnému zamestnancovi umožnený prístup k IKT FS SR,

c) zabezpečí, aby všetky zásahy jej zamestnancov do IKT FS SR boli zaznamenané v protokole z prístupu tretích strán k IKT FS SR. Zamestnanec po ukončení prác súvisiacich s prístupom vyplní tento protokol a ihneď ho e-mailom zašle oprávnenému zamestnancovi a následne mu ho podpísaný zašle aj v písomnej podobe a to do 5 pracovných dní od realizácie prístupu podľa prílohy č. 4.

** Meno kontaktnej osoby za tretiu stranu sa bude uvádzať v žiadosti o prístup externého subjektu k IKT FS SR

5. Záverečné ustanovenia

1. *Všeobecné podmienky* sú záväzné pre tretiu stranu v plnom rozsahu pokiaľ v zmluve nie je ustanovené inak.
2. V prípade porušenia týchto všeobecných podmienok, v dôsledku ktorého vznikne škoda pre FR SR, sa tretia strana zaväzuje nahradiť túto škodu.

3 prílohy

V ..... dňa

_____

štatutárny zástupca tretej strany