Informačno-komunikačná bezpečnosť

(1) Poskytnutie a sprístupnenie IKT aktív

a) Poskytovateľovi budú poskytnuté / sprístupnené nasledujúce aktíva:

1) bezpečnostné zariadenia fyzickej a objektovej ochrany v správe SOMO

2) bezpečnostné zariadenia objektovej ochrany v správe BIT

3) bezpečnostné zariadenia sieťovej ochrany v správe BIT

b) Poskytovateľovi bude umožnený fyzický (mimo ZP), lokálny logický, vzdialený prístup k IKT aktívam uvedeným v predchádzajúcom bode

(2) Pri prístupe k IKT aktívam

a) Poskytovateľ sa zaväzuje v súvislosti s plnením predmetu tejto Zmluvy dodržiavať klasifikáciu informácií ktorá je uvedená v Prílohe č.5 tejto Zmluvy.

b) Poskytovateľ berie na vedomie, že poskytovanie prístupov v rámci siete Objednávateľa, je riadené, monitorované a auditované v súlade s platnou internou dokumentáciou vytvorenou v zmysle odporúčaní normy ISO/IEC 27001.

c) Akceptovateľné použitie informácií / IKT aktív je:

- zhotovovať obrazový záznam IKT aktív len po predchádzajúcom súhlase Manažéra IKT bezpečnosti. Súhlas musí byť vydaný v dokumentovanej podobe,
- pristupovať k P2P sieťam len v správe Objednávateľa,
- mimo prostredia Objednávateľa vynášať IKT zariadenia len so súhlasom oprávneného zamestnanca Objednávateľa. Súhlas musí byť vydaný v dokumentovanej podobe s uvedením dôvodu a dátumu návratu zariadenia, ak sa predpokladá jeho návrat.
- k zariadeniam, ktoré sú pripojené do siete Objednávateľa, pripájať len zariadenia (dátové úložiská: USB kľúče, napaľovačky CD/DVD/BlueRay, externé HDD/SD a pod.; mobilné telefóny a modemy; rôzne sieťové zariadenia: Wi-Fi router, switch, hub, koncové zariadenia s káblovým pripojením: počítače/tablety; ostatné zariadenia: scannery, tlačiarne, fotoaparáty, kamery a pod.), ktoré sú v správe Objednávateľa, alebo boli schválené na používanie v sieti Objednávateľa,
- využívať zariadenia / softvér na prienik do dátových sietí, testovanie zraniteľností, odpočúvanie a zaznamenávanie dátovej komunikácie len po predchádzajúcom súhlase osôb určených Objednávateľom.

d) Neakceptovateľné použitie informácií / IKT aktív je

- využívať pripojenie na Internet na nepracovné účely, s výnimkou využitia nezabezpečenej siete WiFi prevádzkovanej Objednávateľom
- umožniť zariadeniam fyzicky pripojeným do siete Objednávateľa súčasné pripojenie do inej siete (napr. GSM internet, Wi-Fi).

e) Na prístup k IKT aktívam Objednávateľa, uvedeným v bode (1) odstavec a), budú autorizovaní pracovníci Poskytovateľa uvedení v Prílohe č.2 Zmluvy

f) Poskytnutie prístupových práv k IKT aktívu sa vykonáva výhradne na základe Žiadosti o pridelenie / zmenu prístupu k IKT aktívu vlastníkovi IKT aktíva formou e-mailu.

g) Poskytovateľ sa zaväzuje realizovať predmet zmluvy v súlade s požiadavkami IKT bezpečnosti Objednávateľa podľa tejto prílohy

h) Poskytovateľ je povinný preukázateľne oboznámiť svojich pracovníkov s požiadavkami IKT bezpečnosti. Záznam o oboznámení, ktorý bude obsahovať dátum, meno, priezvisko a podpis oboznámeného zamestnanca zašle Objednávateľovi.

i) V prípade výskytu incidentu informačnej bezpečnosti sú kontaktnými osobami za Objednávateľa a za Poskytovateľa osoby uvedené v Prílohe č.2 Zmluvy. V prípade, že v uvedených dokumentoch nie sú explicitne uvedené kontaktné osoby na hlásenie bezpečnostných incidentov, stávajú sa takýmito osobami Odborní garanti Zmluvy Objednávateľa a Poskytovateľa.

(3) Ak má Poskytovateľ fyzický prístup k IKT aktívam Objednávateľa, zaväzuje sa, že počas pobytu v priestoroch Objednávateľa, bude dodržiavať všeobecné zásady bezpečnosti práce, protipožiarnej ochrany a ochrany životného prostredia.

(4) Ak má poskytovateľ prístup k osobným údajom, zaväzuje sa zabezpečiť ochranu osobných údajov v súlade so Zákonom o ochrane osobných údajov.

(5) Ak poskytovateľ realizuje cezhraničný prenos osobných údajov, zaväzuje sa zabezpečiť ochranu osobných údajov v súlade so Zákonom o ochrane osobných údajov, zvlášť ustanovení o cezhraničnom prenose osobných údajov.

(6) Ak bude Poskytovateľ spracovávať informácie mimo siete Objednávateľa, napr. v IS Poskytovateľa (bez ohľadu na miesto inštalácie):

a) Poskytovateľ je povinný zriadiť prístupy k informáciám Objednávateľa umiestneným mimo internej siete Objednávateľa, v rámci zásad najmenších nevyhnutných prístupových práv, ktoré sú potrebné na vykonanie konkrétnej činnosti a všetko je zakázané, ak to nie je výslovne dovolené, pre zabezpečenie nezlučiteľnosti rolí tak, aby zabránil prístupu neautorizovaných osôb k informáciám a aby akékoľvek osoby nezískali nadpráva. Všetky autorizácie na prístup k informáciám musia byť vyhotovené v dokumentovateľnej podobe (písomne / elektronicky / audio záznam / videozáznam). Poskytovateľ je povinný nepretržite monitorovať a na dennej báze vyhodnocovať pokusy o prístupy a raz mesačne písomne informovať Objednávateľa o výsledkoch vyhodnotenia. V prípade zaznamenania neoprávneného prístupu k informáciám je táto skutočnosť považovaná za bezpečnostný incident a zamestnanec Poskytovateľa (uvedený v Prílohe č.2 Zmluvy) o tejto skutočnosti bezodkladne oboznámi kontaktné osoby Objednávateľa (uvedené v Prílohe č.2 Zmluvy).

b) Vlastníkom spracúvaných informácií je Objednávateľ. Informácie sú spracúvané na pracovných staniciach a serveroch Poskytovateľa, ktoré sú umiestnené v prevádzkových priestoroch Poskytovateľa, ktoré slúžia na plnenie predmetu Zmluvy. Poskytovateľ je povinný zabezpečiť ochranu spracúvaných informácií pred ich stratou a vyzradením.

c) Objednávateľ si vyhradzuje právo vykonávať audit poskytovateľových procesov a opatrení v oblasti informačnej bezpečnosti na zariadeniach a v priestoroch Poskytovateľa, ktoré slúžia na plnenie predmetu Zmluvy. Objednávateľ sa zaväzuje pri výkone auditu nenarušiť závažným spôsobom prevádzku Poskytovateľa

(7) Predmetom Zmluvy nie je dodávka zariadenia.

(8) Popis poskytovaných služieb je súčasťou Zmluvy – Príloha č. 1.

(9) Ak predmetom Zmluvy je vytvorenie, aktualizácia, alebo inštalácia informačného systému, ktorý bude komunikovať s inými informačnými systémami Objednávateľa, resp. ak predmetom Zmluvy bude prepojenie iného informačného systému s informačnými systémami Objednávateľa, Poskytovateľ vyhotoví podrobný popis technického riešenia, pripojenia a spôsobu komunikácie predmetu Zmluvy s týmito informačnými systémami.

Ak uvedená komunikácia prebiehajúca formou vzájomných transakcií aplikačných služieb bude prebiehať v rámci internej infraštruktúry Objednávateľa, alebo prostredníctvom verejných sietí, tento technický popis dodaný Poskytovateľom bude okrem iného obsahovať:

a) spôsob využitia verejného/súkromného kľúča, alebo elektronického podpisu na overenie identity druhej strany,

b) spôsob overovania platnosti autentifikácie druhej strany,

c) spôsob zabezpečovanie dôvernosti a integrity transakcie,

d) spôsob autorizácie všetkých vykonaných úkonov,

e) spôsob používania zabezpečených protokolov na báze SSL/TLS vo vzájomnej komunikácii,

f) spôsob zabezpečenia úložiska transakčných podrobností (zabezpečenia dôvernosti a integrity transakčných dokumentov jeho umiestnením mimo akéhokoľvek dosiahnuteľného prostredia neoprávnenými osobami),

g) v prípade využívania dôveryhodnej autority (napr. na účely vydávania a údržby elektronického podpisu, alebo digitálnych certifikátov) zvýraznenie integrácie bezpečnosti v celom procese riadenia certifikátov a podpisov od začiatku do konca

(10) Poskytovateľ je na plnenie predmetu Zmluvy oprávnený využiť Subdodávateľov na ktorých sa vzťahujú rovnaké požiadavky IKT bezpečnosti ako na Poskytovateľa. Za ich splnenie zodpovedá Poskytovateľ.

(11) Zmluvné strany sa dohodli, že prenos informácií sa bude realizovať v papierovej a elektronickej podobe. Elektronické informácie budú odosielané vo vopred dohodnutom formáte, pred ich odoslaním budú skontrolované, či neobsahujú malvér (škodlivý kód) a počas prenosu s nimi bude narábané v súlade s Prílohou č. 4 Zmluvy

(12) Zmluvné strany sa dohodli, že v prípade prenosu informácií na fyzickom médiu budú tieto zaznamenané na fyzickom médiu v dohodnutom formáte, a toto médium bude v zmysle Prílohy č. 4 Zmluvy označené triedou klasifikácie, nosiče budú zabalené ako Poistená zásielka Slovenskej pošty, prípadne porovnateľný produkt iného poštového operátora a budú ich prepravovať dôveryhodní kuriéri, ktorí sa adresátovi preukážu. Adresát potvrdí kuriérovi prevzatie neporušeného nosiča svojim podpisom na sprievodnom liste.

(13) Neprerušiteľnosť spracovania:

Poskytovateľ je povinný realizovať predmet Zmluvy tak, aby nedošlo k prerušeniu, alebo obmedzeniu prevádzky Objednávateľa. V prípade, ak plnenie predmetu Zmluvy nevyhnutne vyžaduje prerušenie alebo obmedzenie prevádzky Objednávateľa, je Poskytovateľ povinný vopred preukázateľne o tejto skutočnosti informovať Objednávateľa a do doby, pokiaľ Poskytovateľ nedostane inštrukcie od Objednávateľa o ďalšom postupe, alebo súhlas s plnením predmetu Zmluvy, je Poskytovateľ povinný zdržať sa takého vykonávania predmetu Zmluvy, ktoré by mohlo spôsobiť prerušenie, alebo obmedzenie prevádzky Objednávateľa. V opačnom prípade zodpovedá Poskytovateľ za škody, ktoré týmto spôsobí Objednávateľovi.

Objednávateľ je oprávnený odstúpiť od Zmluvy, ak poskytovateľ nemôže plniť požiadavky IKT bezpečnosti, uvedené v tejto prílohe, vo vlastnej réžii resp. prostredníctvom subdodávateľa.

V prípade zániku poskytovateľa bez právneho nástupcu je poskytovateľ povinný odovzdať objednávateľovi vytvorenú projektovú dokumentáciu, funkčné špecifikácie a analytické materiály. Pokiaľ existujú, tak aj vytvorené zdrojové kódy.

(14) Vrátenie aktív:

Zmluvné strany sú povinné po zániku tejto Zmluvy:

a) v lehote 60 dní od zániku tejto Zmluvy vrátiť druhej zmluvnej strane všetky fyzické a elektronické aktíva patriace tejto zmluvnej strane, ktoré im boli v súvislosti s plnením predmetu tejto Zmluvy poskytnuté; to neplatí ak v rovnakej lehote bude uzatvorená alebo je v rokovacom konaní nová zmluva medzi stranami s rovnakým alebo podobným predmetom plnenia ako je táto Zmluva

b) v lehote 60 dní od zániku tejto Zmluvy zabezpečiť bezpečné odstránenie elektronických aktív druhej zmluvnej strany v prípade, ak sú elektronické aktíva patriace jednej zmluvnej strane v súvislosti s plnením predmetu tejto Zmluvy umiestnené na zariadení druhej zmluvnej strany; to neplatí ak v rovnakej lehote bude uzatvorená alebo je v rokovacom konaní nová zmluva medzi stranami s rovnakým alebo podobným predmetom plnenia ako je táto Zmluva

(15) Ak sa predpokladajú zmeny v predmete Zmluvy (napr. vývoj softvéru):

Kontaktnými osobami pre riadenie zmien sú zamestnanci uvedení v Prílohe č.1 tejto Zmluvy.

(16) Pri zistení porušenia niektorých z bezpečnostných požiadaviek uvedených v tejto prílohe Zmluvy a v prípade, že zistený nedostatok nebude odstránený ani na základe písomnej výzvy Objednávateľa a poskytnutí primeranej lehoty na jej odstránenie, je objednávateľ oprávnený odstúpiť od Zmluvy.

(17) Poskytovateľ sa zaväzuje urobiť opatrenia, aby:

a) pri plnení jeho záväzkov podľa tejto Zmluvy nedochádzalo z jeho strany k porušovaniu licenčných pravidiel platných pre písomne odsúhlasené alebo v tejto Zmluve uvedené verzie operačných systémov, databázového prostredia a ďalších podporných a integračných softvérov, slúžiacich pre prevádzku aplikačného softvéru Objednávateľa, ktorého dodávka/úprava/podpora je predmetom záväzku Poskytovateľa podľa tejto Zmluvy, alebo ktorého sa týka poskytnutie služieb v zmysle tejto Zmluvy (ďalej len pravidlá licenčnej politiky) a

b) aby plnenie, ktoré objednávateľovi na základe tejto Zmluvy poskytne, neporušovalo pravidlá licenčnej politiky.

Ak sa preukáže porušenie pravidiel licenčnej politiky, ktoré bolo spôsobené činnosťou Poskytovateľa, Poskytovateľ sa zaväzuje uhradiť Objednávateľovi všetky náhrady škody prípadne všetky iné finančné náklady, ktoré Objednávateľovi vzniknú v dôsledku takéhoto porušenia pravidiel licenčnej politiky Poskytovateľom a budú uplatnené autorom softvéru prípadne inou oprávnenou osobou voči Objednávateľovi. Akákoľvek limitácia náhrady škody dohodnutá v tejto Zmluve sa nevzťahuje na náhradu škody, ktorú je Poskytovateľ povinný zaplatiť Objednávateľovi v zmysle tohto bodu Zmluvy. Povinnosť nahradiť vzniknutú škodu alebo iné finančné náklady, ktoré Objednávateľovi vzniknú v dôsledku porušenia pravidiel licenčnej politiky Poskytovateľom trvá aj po ukončení platnosti tejto Zmluvy a to aj v prípade, ak bol nárok na ich zaplatenie uplatnený voči Objednávateľovi po ukončení platnosti tejto Zmluvy.

(18) Dokumentácia dodávaná Poskytovateľom k plneniam podľa tejto Zmluvy bude klasifikovaná v súlade s Prílohou č. 4. Zmluvy dohodou zmluvných strán.

Vo všeobecnosti platí, že bežná používateľská dokumentácia, ktorá neobsahuje prístupové údaje k informačným systémom (mená, kontá, heslá) a iné citlivé informácie, je klasifikovaná v triede „interné“.

Administrátorská a obdobná dokumentácia, ktorá obsahuje inštalačné a konfiguračné postupy, citlivé prístupové údaje a vyhradené informácie, je klasifikovaná v triede „chránené“.

Objednávateľom preferovaný formát dokumentácie je docx/doc, alternatívny formát je pdf.