Asseco CEIT, a. s.
info@asseco-ceit.com
Univerzitná 8661/6A, 010 08 Žilina
Slovenská republika
+421 (0)41 513 7401
+421 (0)41 513 9290

Pravidlá pre bezpečnostne významných dodávateľov

S bezpečnostne významným dodávateľom musí byť uzatvorená NDA (Non-Disclosure Agreement) zaväzujúca dodržiavanie dôvernosti a bezpečnosti poskytnutých informácií, dokumentov a zariadení. V prípade porušenia tejto zmluvy je dodávateľ povinný znášať dôsledky vyplývajúce z tejto zmluvy (zmluvná pokuta, náhrada škody).
Dodávateľ musí mať zavedený systém riadenia bezpečnosti informácií (certifikácia nie je vyžadovaná).

a) Vytvoriť a schváliť bezpečnostnú politiku, ktorá bude pokrývať zabezpečenie dát a informácií, ktoré môžu byť vytvárané a spracovávané na strane dodávateľa pri poskytovaní predmetu plnenia. Bezpečnostná politika musí obsahovať hlavné zásady, ciele, bezpečnostné potreby, práva a povinnosti vo vzťahu k riadeniu bezpečnosti informácií.
b) Riadiť vlastné riziká, ktoré môžu ovplyvniť poskytovanie predmetu plnenia.
c) Na základe bezpečnostných potrieb a výsledkov hodnotenia rizika zaviesť príslušné bezpečnostné opatrenia v rozsahu poskytovaného predmetu plnenia, monitorovať ich, vyhodnocovať ich účinnosť.
d) Stanoviť a udržiavať aktuálne opatrenia bezpečnosti vo forme procesov a technológií, ktoré zaisťujú naplnenie bezpečnostnej politiky.
e) Viesť záznamy o vytváraní a spracovaní dát a informácií v rozsahu poskytovaného predmetu plnenia, zaznamenávať všetky podstatné okolnosti súvisiace so zaistením bezpečnosti týchto dát a informácií a na požiadanie tieto záznamy spoločnosti Asseco CEIT, a. s. sprístupniť.
f) Ak využíva pri poskytovaní predmetu plnenia subdodávateľa, zabezpečiť adekvátne dodržiavanie týchto bezpečnostných požiadaviek aj v zmluvných vzťahoch so svojimi subdodávateľmi.

1 Bezpečnosť ľudských zdrojov

1.1 Bezpečnostne významný dodávateľ a jeho prípadní subdodávatelia majú povinnosť vo svojich interných procesoch zabezpečiť nasledujúce opatrenia:

a) má zavedený plán rozvoja bezpečnostného povedomia, ktorého cieľom je zabezpečiť primeranú vzdelávanie a zlepšovanie bezpečnostného povedomia a ktorý obsahuje:
    - poučenie používateľov, administrátorov, osôb zastávajúcich bezpečnostné role a subdodávateľov o ich povinnostiach a o bezpečnostnej politike;
    - absolvovanie teoretických aj praktických školení užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role;
b) má určené osoby zodpovedné za realizáciu jednotlivých činností, ktoré sú v pláne uvedené;
c) v súlade s plánom rozvoja bezpečnostného povedomia zabezpečuje poučenie používateľov, administrátorov, osôb zastávajúcich bezpečnostné role a dodávateľov o ich povinnostiach a o bezpečnostnej politike formou vstupných a pravidelných školení;
d) pre osoby zastávajúce bezpečnostné úlohy v súlade s plánom rozvoja bezpečnostného povedomia zabezpečuje pravidelné odborné školenia, pričom vychádza z aktuálnych potrieb v oblasti kybernetickej bezpečnosti;

e) v súlade s plánom rozvoja bezpečnostného povedomia zabezpečuje pravidelné školenia a overovanie bezpečnostného povedomia zamestnancov v súlade s ich pracovnou náplňou;
f) zabezpečuje kontrolu dodržiavania bezpečnostnej politiky zo strany používateľov, administrátorov a osôb zastávajúcich bezpečnostné role;
g) v prípade ukončenia zmluvného vzťahu s administrátormi a osobami zastávajúcimi bezpečnostné role zaisťuje prenos zodpovednosťou;
h) určuje pravidlá a postupy riešenia prípadov porušenia stanovených bezpečnostných pravidiel zo strany používateľov, administrátorov a osôb zastávajúcich bezpečnostné role;
i) vedie o vykonaných školení prehľady, ktoré obsahujú predmet školenia a zoznam osôb, ktoré školenie absolvovali.

1.2 Asseco CEIT, a.s. si vyhradzuje právo viesť záznamy a preverovať činnosti dodávateľa, viesť záznamy o incidentoch a neštandardných činnostiach zamestnancov a iných osôb pôsobiacich v prospech dodávateľa. Na základe týchto záznamov má oprávnenie vyhodnocovať dôveryhodnosť a spoľahlivosť zamestnancov dodávateľa. V prípade zisteného rizika oznámi Asseco CEIT, a.s. nesúlad dodávateľmi a obe strany vojdú v rokovaní na riešenie tejto situácie.

1.3 Kvalifikácia zamestnancov dodávateľa musí zodpovedať vykonávanej pracovnej pozícii (vykonávanej práci a úrovni zabezpečenia).

2 Fyzická bezpečnosť, protipožiarna ochrana a BOZP

Dodávateľ ako zamestnávateľ pri vykonávaní prác pri plnení predmetu plnenia zodpovedá za dodržiavanie predpisov BOZP a PO svojimi zamestnancami, popr. ďalšími fyzickými osobami vykonávajúcimi prácu v jeho prospech a zodpovedá za dodržiavanie podmienok vstupu osôb do objektov Asseco CEIT, a.s.

3 Riadenie prevádzky IS

Dodávateľ sa zaväzuje:

a. Zabezpečiť bezpečnú prevádzku informačného systému a infraštruktúry využívané na poskytovanie predmetu plnenia.
b. Na vyžiadanie poskytnúť Asseco CEIT, a.s. prehľad o bezpečnostných opatreniach zavedených na svojom informačnom systéme a infraštruktúre, v ktorej plnia predmet zmluvy.
c. Zabezpečiť, že pre poskytovanie predmetu plnenia budú využívané iba aplikácie a technológie, ktoré sú v súlade s platnou slovenskou a európskou legislatívou, predovšetkým s ohľadom na licenčné podmienky, autorské práva a práva súvisiace s právom autorským a o zmene niektorých zákonov (autorský zákon) v znení neskorších predpisov.

4 Riadenie prístupov

4.1 Identifikácia:

a. Každý zamestnanec dodávateľa podieľajúce sa na plnení zmluvy výpočtovými prostriedkami dodávateľa, musí mať v rámci svojej IT infraštruktúry evidovaný a vedený svoj vlastný jedinečný užívateľský účet, ktorému sú v jednotlivých určených systémoch, moduloch alebo aplikáciách priradené špecifické roly. Každý zamestnanec dodávateľa musí byť vedený s platnými identifikačnými a aktuálnymi kontaktnými údajmi.
b. Každý zamestnanec dodávateľa, ak pristupuje k interným systémom Asseco CEIT, a.s., má v Asseco CEIT, a.s. vytvorený jedinečný užívateľský účet, ktorému sú v jednotlivých systémoch, moduloch alebo aplikáciách priradené špecifické roly súvisiace výlučne s plnením predmetu zmluvy.

4.2 Autentifikácia

4.2.1 Podmienky pre autentizáciu pri využití ICT infraštruktúry Asseco CEIT, a.s.

a. na jednoznačnú identifikáciu privilegovaných užívateľov určených systémov sa využíva viacfaktorová autentizácie.
b. overenie heslom - ak nie je možné použiť jednoznačnú identifikáciu privilegovaných užívateľov viac faktormi, je použitá autentizácia pomocou kryptografických kľúčov so zaručením obdobnej úrovne bezpečnosti alebo použitie hesla s vyžadovanými pravidlami.

4.2.2 Pre vzdialený prístup zamestnancov dodávateľa predkladá dodávateľ podklady pre vyplnenie žiadosti o vzdialený prístup, podľa ktorej sú potom nastavené parametre bezpečného vzdialeného prístupu.

a. za dodávateľa žiadosť interne v Asseco CEIT, a.s. vypĺňa zodpovedná osoba príslušného určeného systému Asseco CEIT, a.s. (Na základe podkladov od kontaktnej osoby dodávateľa).
b. po spracovaní žiadosti je zamestnanec dodávateľa individuálne oboznámený s detailmi pravidiel vzdialeného prístupu a sú mu odovzdané autentizačné údaje.

4.2.3 Dodávateľ zodpovedá za činnosti svojich zamestnancov, prípadne ďalších fyzických osôb zamestnaných v jeho prospech, ktoré musia byť v súlade bezpečnostnými pravidlami a ďalšími upresňujúcimi bezpečnostnými informáciami preukázateľne odovzdanými zo strany Asseco CEIT, a.s. na základe vyžiadanie zo strany dodávateľa. Všetky škody, ktoré vzniknú porušením týchto a ďalších spresňujúcich bezpečnostných informácií zamestnanci dodávateľa alebo ďalšími osobami vykonávajúcimi prácu v jeho prospech, idú na ťarchu dodávateľa, ktorý je povinný tieto škody v plnom rozsahu Asseco CEIT, a.s. nahradiť.

4.3 Autorizácia

4.3.1 Zamestnanci dodávateľa sú povinní v ICT infraštruktúre Asseco CEIT, a.s. využívať privilegované oprávnenia len v primeranej miere a len po dobu nevyhnutne potrebnú na vykonanie činností v súlade s plnením predmetu zmluvy. Užívatelia ani administrátori nesmú používať účty s privilegovanými privilégiami pre bežnú prácu nesúvisiace so správou určeného systému.

4.3.2 Zamestnanci dodávateľa sú informovaní Asseco CEIT, a.s., ku ktorým chráneným informáciám Asseco CEIT, a.s. majú prístup a ako s nimi môžu nakladať. Akékoľvek manipulácie a ďalšie operácie s

chránenými informáciami Asseco CEIT, a.s., ktoré neboli výslovne v inštrukciách uvedené, nemá dodávateľ povolené.

4.4 Podmienky vzdialeného prístupu
4.4.1 Pre prístup k informačným systémom Asseco CEIT, a.s. sú štandardne použité prostriedky Asseco CEIT, a.s. (HW, SW). Prístup výpočtovej techniky dodávateľa (PC, notebooky) k chráneným interným informáciám a k informačným a telekomunikačným systémom je podmienený schválením IKT oddelenia Asseco CEIT, a.s. a zodpovedným administrátorom (garantom) systému.

4.4.2 Pracovné stanice dodávateľa prichádzajúci prostredníctvom VPN musí:

a. mať pokročilú funkčnú antivírusovú ochranu (so zapnutou ochranou v reálnom čase);
b. mať funkčný osobný firewall;
c. mať nastavené automatické/spravované aktualizácie operačného systému;
d. mať operačný systém, ktorý nie je mimo servisnú podporu;
e. mať v Linux prostredí zaistené podobné podmienky ako vyššie definované pre Windows - AV, FW, UPDATE, OS.;
f. uložiť do koncovej stanice identifikačné a autorizačné prvky poskytnuté určeným zamestnancom Asseco CEIT, a.s.;
g. mať nainštalovaného VPN klienta, inštalované čisto v réžii dodávateľa;
h. mať druhý faktor (HW alebo SMS token) pre prístup k VPN, ten bude poskytnutý určeným zamestnancom;
i. mať aktualizované aplikácie tretích strán bez porušovania autorských práv.

5 Riadenie zmien

Zmeny na strane dodávateľa musí byť riadené s ohľadom na kritickosť informácií, systémov, procesov a opätovným posudzovaním rizík. Dodávateľ sa zaväzuje:

a) Riadiť a evidovať zmluvné zmeny.
b) Riadiť a evidovať zmeny v poskytovaných službách v súlade s odporúčaniami štandardov informačnej bezpečnosti.

6 Akvizícia, vývoj, údržba

Dodávateľ sa zaväzuje zabezpečiť bezpečnú implementáciu, inováciu, aktualizáciu, testovanie technológií, ktoré sú predmetom plnenia a odovzdať Asseco CEIT, a.s. dokumentáciu predmetu plnenia minimálne v nasledujúcom rozsahu:

a) dokumentáciu skutočného vyhotovenia,
b) dokumentáciu všetkých bezpečnostných nastavení, funkcií a mechanizmov,
c) dokumentáciu obsahujúcu popis autorizačného konceptu a oprávnenia,
d) dokumentáciu obsahujúcu zálohovacie a archivačné postupy,
e) dokumentáciu obsahujúcu inštalačné a konfiguračné postupy

f) dokumentáciu zahŕňajúce testy zraniteľností a súlad s bezpečnostnými požiadavkami Asseco CEIT, a.s.
g) dokumentáciu pre zabezpečenie kontinuity prevádzky a obnovy po havárii.

V prípade vývoja riešení sa dodávateľ zaväzuje:

a. Dodržiavať a implementovať najlepšie praktiky pre bezpečný vývoj softvéru.
b. Ak je odovzdanie zdrojového kódu k riešeniu súčasťou plnenia podľa zmluvy, bude umožnený audit vykonávaného alebo vykonaného plnenia, a to najmä s cieľom overiť, či sa postupovalo podľa plnenia v súlade so zmluvou.
c. Zabezpečiť, že plnenie bude obsahovať len tie súčasti, ktoré sú objektívne potrebné pre riadne prevádzkovanie riešenia a / alebo ktoré sú špecifikované výslovne v zmluve (najmä, že riešenie nebude obsahovať žiadne nepotrebné komponenty, žiadne programové vzorky a pod.).
d. Pokiaľ je súčasťou plnenia aj inštalácia operačného systému prípadne softvéru tretích strán, zabezpečiť v priebehu jeho inštalácie, že budú použité predpísané verzie týchto produktov kompatibilný a funkčný v prostredí Asseco CEIT, a.s.
e. Zabezpečiť bezpečnosť testovacieho prostredia u dodávateľa a ochranu poskytnutých testovacích dát Asseco CEIT, a.s.
f. Zabezpečiť, že v produkčnom prostredí Asseco CEIT, a.s. bude dodaný len predmetom zmluvy špecifikovaný kompilovaný, respektíve spustiteľný kód a ďalšie potrebné údaje na prevádzkovanie predmetu plnenia
g. Zabezpečiť, že v rámci poskytovaného plnenia bude dodávané riešenie v súlade s odporúčaniami štandardov informačnej bezpečnosti.
h. Poskytnúť objednávateľovi potrebnú súčinnosť v prípade, že objednávateľ vyžaduje / realizuje prevedenie bezpečnostných testov súvisiacich s predmetom plnenia. V prípade, že objednávateľ požaduje od dodávateľa potvrdenie o vykonaní bezpečnostných testov, bude uvedené dohodnuté samostatnou zmluvnou dohodou.
i. Odovzdať zdrojový kód Asseco CEIT, a.s., ak je to uvedené v zmluve, bezpečnou formou so zaistením jeho integrity.
j. Zabezpečiť riadenie verzií zdrojového kódu.
k. Zabezpečiť zálohovanie zdrojového kódu a jeho uloženie mimo produkčné prostredie.
l. Zabezpečiť, aby distribúcia zdrojových kódov obsahovala súbor z vývojového prostredia na riadenú kompiláciu týchto zdrojových kódov
m. nevyvíjať, nekompilovať a nešíriť v prostredí Asseco CEIT, a.s. programový kód, ktorý má za cieľ nelegálne ovládnutie, narušenie dostupnosti, dôvernosti alebo integrity alebo neautorizované či nelegálne získanie dát a informácií.

7 Monitoring

a) Prístup zamestnancov dodávateľa k vybraným chráneným interným informáciám a k informačným a komunikačným systémom Asseco CEIT, a.s. je nepretržite zaznamenávaný,

monitorovaný a vyhodnocovaný. Udalosti v systémoch sú Asseco CEIT, a.s. zaznamenávané do logov.

b) Dodávateľ je povinný priebežne monitorovať v rámci svojej IKT infraštruktúry zverejnené a známe bezpečnostné chyby, ktoré môžu ovplyvniť hladký a bezpečnú prevádzku systémov súvisiacich s ním poskytovanými službami. Jedná sa napríklad o zraniteľnosti v operačných systémoch, softvér tretích strán, webové komponenty atď.

8 Ochrana médií

a. Uloženie chránených informácií Asseco CEIT, a.s. na prenosné médiá a prípadný transport médií mimo priestorov Asseco CEIT, a.s. podlieha jeho schváleniu.
b. V prípade ukladania chránených informácií Asseco CEIT, a.s. na prenosné médiá je dodávateľ povinný, ak je to technicky možné, ukladať, prípadne vyžadovať uloženie týchto dát v šifrovanej podobe a viesť evidenciu týchto médií.
c. Dodávateľ je povinný zabezpečiť likvidáciu operatívnych dát obsahujúcich chránené informácie Asseco CEIT, a.s. ihneď po pominutí účelu ich spracovania a/alebo uloženia. Po likvidácii dát na elektronickom médiu nesmie byť možné informáciu obnoviť. O vykonaní likvidácie dát musí dodávateľ viesť protokol.

9 Kybernetické incidenty

Dodávateľ má za povinnosť hlásiť všetky podozrenia na kybernetické incidenty:

a. zodpovednej osobe Asseco CEIT, a.s.
b. v termíne bezprostredne (bez omeškania) po zistení kybernetickej bezpečnostné udalosti / incidentu.
c. formou emailu, telefonicky so zaistením evidencia hovoru na oboch stranách, alebo osobne.
d. s popisom:
    - dátumu a času zistenia incidentu;
    - povahy udalosti;
    - zdroja udalosti;
    - ciele / obete udalosti;
    - potencionálnym vplyvom.

10 Zákaznícky audit

10.1 Oprávnenie na vykonanie auditu

a. Asseco CEIT, a.s. si vyhradzuje právo vykonávať audity dodávateľa.
b. Asseco CEIT, a.s. s dostatočným predstihom aspoň 5 pracovných dní oznámi dodávateľovi zámer na vykonanie auditu. Obe strany si dohodnú obsah, potrebnú súčinnosť a časový plán auditu s tým, že Asseco CEIT, a.s. sa zaväzuje postupovať tak, aby nenarušil prevádzkové potreby dodávateľa.

c. Asseco CEIT, a.s. si vyhradzuje právo v prípade závažných dôvodov (napr. podozrenie na rizikové správanie dodávateľa) v súvislosti s plnením zmluvy vykonať neohlásený audit u dodávateľa s prihliadnutím na prevádzkovú situáciu dodávateľa.
d. Audítor/inšpektor ustanovuje pri zistení nezhôd nápravné opatrenia na zistenie a dátum ich zavedenia. Dodávateľ je povinný nápravné opatrenia realizovať v rozsahu stanoveného opatrenia a v požadovanom termíne.
e. Dokumentácia auditov vykonaných Asseco CEIT, a.s. je vedená v útvare zodpovednom za vykonávanie auditov. Záznamy týkajúce sa určitého auditu sú vždy označované rovnakým identifikátorom. Jednotlivé záznamy auditov tvoria:
    - plán auditu;
    - oznámenie o audite;
    - dotazník k auditu (zoznam otázok audítora, ak audítor uzná za vhodné);
    - správa z auditu;
    - písomné, fotografické alebo iné záznamy prevádzky, postupov alebo zariadení, ktoré súvisia s auditom (pokiaľ je nevyhnutné pre dokumentovanie nálezov);
    - záznam o zistení (nápravných opatreniach a následnej kontrole).

f. Auditovaná strana (dodávateľ) obdrží na vyjadrenie záverečnú správu auditu obsahujúcu prípadné zistenia:
    - dodávateľ navrhne na základe zistení uvedených v záverečnej audítorskej správe návrh opatrení a termíny riešenie a odovzdá ich zoznam Asseco CEIT, a.s. na odsúhlasenie;
    - Asseco CEIT, a.s. potvrdí súhlas s navrhovanými opatreniami.

10.2 Nápravné opatrenia

a. Auditovaná strana (dodávateľ) má za povinnosť v určenom čase zabezpečiť realizáciu dohodnutých nápravných opatrení.
b. Správu o realizovaných opatreniach dodávateľ oznamuje a odovzdáva Asseco CEIT, a.s.

11 Ochrana aktív proti neautorizovaným činnostiam

Dodávateľ na aktíva Asseco CEIT, a. s. neinštaluje a nepoužíva nástroje, ktoré nie sú súčasťou predmetu plnenia.

12 Podmienky ukončenia zmluvy

a. V prípade ukončenia zmluvného vzťahu musí byť ukončené všetky prístupy dodávateľa a jeho zamestnancov k aktívam Asseco CEIT, a.s. (VPN, systémy, informácie) najneskôr k termínu ukončenia zmluvného vzťahu.
b. Ak boli zamestnancom dodávateľa poskytnuté aktíva Asseco CEIT, a.s. musia byť tieto aktíva vrátené najneskôr k termínu ukončenia zmluvného vzťahu.

c. Ak zhotoviteľom boli poskytnuté informačné aktíva (dáta) Asseco CEIT, a.s. musia byť najneskôr k termínu ukončenia zmluvného vzťahu vrátené a bezo zvyšku zmazané, bez možnosti obnovenia zo všetkých systémov dodávateľa a nosičov dodávateľa.
d. V prípade predčasného ukončenia zmluvného vzťahu iným spôsobom ako splnením záväzku (napr. výpoveďou, odstúpením od zmluvy, dohodou o ukončení zmluvy a pod.), môžu byť prístupy dodávateľa, ak je to potrebné, zo strany Asseco CEIT, a.s. ukončené pred uplynutím doby trvania zmluvného vzťahu.