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

Pravidla pro bezpečnostně významné dodavatele

S bezpečnostně významným dodavatelem musí být uzavřena smlouva o mlčenlivosti (NDA, Non-Disclosure Agreement) zavazující dodržování důvěrnosti a zabezpečení poskytnutých informací, dokumentů a zařízení. V případě porušení této smlouvy je dodavatel povinen nést důsledky vyplývající z této smlouvy (smluvní pokuta, náhrada škody).
Dodavatel musí mít zavedený systém řízení bezpečnosti informací (certifikace není vyžadována).

a) Vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, které mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
b) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
c) Na základě bezpečnostních potřeb a výsledků hodnocení rizika zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
d) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
e) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat všechny podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na požádání tyto záznamy zpřístupnit společnosti Asseco CEIT, a. s.
f) Využívá-li při poskytování předmětu plnění subdodavatele, zajistit adekvátní dodržování těchto bezpečnostních požadavků i ve smluvních vztazích se svými subdodavateli.

1 Bezpečnost lidských zdrojů

1.1 Bezpečnostně významný dodavatel a jeho případní subdodavatelé mají povinnost ve svých interních procesech zajistit následující opatření:

a) mít zaveden plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit přiměřené vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje:
   - poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a subdodavatelů o jejich povinnostech a o bezpečnostní politice;
   - absolvování teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;
b) mít určené osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;
c) v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
d) pro osoby zastávající bezpečnostní úkoly v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná odborná školení, přičemž musí vycházet z aktuálních potřeb v oblasti kybernetické bezpečnosti;

e) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
f) zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
g) v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťovat přenos odpovědností;
h) určovat pravidla a postupy řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
i) vést o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.2 Asseco CEIT, a.s. si vyhrazuje právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a jiných osob působících ve prospěch dodavatele. Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele. V případě zjištěného rizika oznámí Asseco CEIT, a.s. nesoulad ze strany dodavatelů a obě strany zahájí v jednání za účelem řešení této situace.

1.3 Kvalifikace zaměstnanců dodavatele musí odpovídat vykonávané pracovní pozici (vykonávané práci a úrovni zabezpečení).

2 Fyzická bezpečnost, protipožární ochrana a BOZP

Dodavatel jako zaměstnavatel při vykonávání prací při plnění předmětu plnění zodpovídá za dodržování předpisů BOZP a PO svými zaměstnanci, příp. jinými fyzickými osobami vykonávajícími práci v jeho prospěch, a zodpovídá za dodržování podmínek vstupu osob do objektů Asseco CEIT, a.s.

3 Řízení provozu IS

Dodavatel se zavazuje:

a. Zabezpečit bezpečný provoz informačního systému a infrastruktury využívané k poskytování předmětu plnění.
b. Na vyžádání poskytnout Asseco CEIT, a.s. přehled o bezpečnostních opatřeních zavedených ve svém informačním systému a infrastruktuře, ve které plní předmět smlouvy.
c. Zabezpečit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou slovenskou a evropskou legislativou, především s ohledem na licenční podmínky, autorská práva a práva související s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

4 Řízení přístupů

4.1 Identifikace:

a. Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele musí mít v rámci své IT infrastruktury evidovaný a vedený svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých určených systémech, modulech nebo aplikacích přiřazeny konkrétní role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.
b. Každý zaměstnanec dodavatele, pokud přistupuje k interním systémům Asseco CEIT, a.s., má v Asseco CEIT, a.s. vytvořen jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny konkrétní role související výlučně s plněním předmětu smlouvy.

4.2 Autentizace

4.2.1 Podmínky pro autentizaci při využití ICT infrastruktury Asseco CEIT, a.s.

a. k jednoznačné identifikaci privilegovaných uživatelů určených systémů se využívá vícefaktorová autentizace.
b. ověření heslem – není-li možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s vyžadovanými pravidly.

4.2.2 Pro vzdálený přístup zaměstnanců dodavatele předkládá dodavatel podklady pro vyplnění žádosti o vzdálený přístup, podle které jsou pak nastaveny parametry bezpečného vzdáleného přístupu.

a. za dodavatele žádost interně v Asseco CEIT, a.s. vyplňuje odpovědná osoba příslušného určeného systému Asseco CEIT, a.s. (Na základě podkladů od kontaktní osoby dodavatele).
b. po zpracování žádosti je zaměstnanec dodavatele individuálně obeznámen s podrobnostmi pravidel vzdáleného přístupu a jsou mu předány autentizační údaje.

4.2.3 Dodavatel odpovídá za činnosti svých zaměstnanců, případně dalších fyzických osob zaměstnaných v jeho prospěch, které musí být v souladu bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany Asseco CEIT, a.s. na základě vyžádání ze strany dodavatele. Veškeré škody, které vzniknou porušením těchto a dalších upřesňujících bezpečnostních informací zaměstnanci dodavatele nebo dalšími osobami vykonávajícími práci v jeho prospěch, jdou k tíži dodavatele, který je povinen tyto škody v plném rozsahu Asseco CEIT, a.s. nahradit.

4.3 Autorizace

4.3.1 Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře Asseco CEIT, a.s. využívat privilegovaných oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou k provedení činností v souladu s plněním předmětu smlouvy. Uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou určeného systému.

4.3.2 Zaměstnanci dodavatele jsou informováni Asseco CEIT, a.s., ke kterým chráněným informacím Asseco CEIT, a.s. mají přístup a jak s nimi mohou nakládat. Jakékoliv manipulace a další operace s chráněnými informacemi Asseco CEIT, a.s., které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povolené.

4.4 Podmínky vzdáleného přístupu

4.4.1 Pro přístup k informačním systémům Asseco CEIT, a.s. jsou standardně používány prostředky Asseco CEIT, a.s. (HW, SW). Přístup výpočetní techniky dodavatele (PC, notebooky) k chráněným interním informacím a k informačním a telekomunikačním systémům je podmíněn schválením IKT oddělení Asseco CEIT, a.s. a odpovědným administrátorem (garantem) systému.

4.4.2 Pracovní stanice dodavatele přicházející prostřednictvím VPN musí:

a. mít pokročilou funkční antivirovou ochranu (se zapnutou ochranou v reálném čase);
b. mít funkční osobní firewall;
c. mít nastaveny automatické/spravované aktualizace operačního systému;
d. mít operační systém, který není mimo servisní podporu;
e. mít v Linux prostředí zajištěny podobné podmínky jako výše definované pro Windows – AV, FW, UPDATE, OS.;
f. uložit do koncové stanice identifikační a autorizační prvky poskytnuté určeným zaměstnancům Asseco CEIT, a.s.;
g. mít nainstalovaného VPN klienta; instalace spadá čistě do režie dodavatele;
h. mít druhý faktor (HW nebo SMS token) pro přístup k VPN, který bude poskytnut určeným zaměstnancům;
i. mít aktualizované aplikace třetích stran bez porušování autorských práv.

5 Řízení změn

Změny na straně dodavatele musí být řízené s ohledem na kritičnost informací, systémů, procesů a opětovným posouzením rizik. Dodavatel se zavazuje:

a) Řídit a evidovat smluvní změny.
b) Řídit a evidovat změny v poskytovaných službách v souladu s doporučeními standardů informační bezpečnosti.

6 Akvizice, vývoj, údržba

Dodavatel se zavazuje zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění a předat Asseco CEIT, a.s. dokumentaci předmětu plnění minimálně v následujícím rozsahu:

a) dokumentaci skutečného provedení,
b) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů,
c) dokumentaci obsahující popis autorizačního konceptu a oprávnění,
d) dokumentaci obsahující zálohovací a archivační postupy,
e) dokumentaci obsahující instalační a konfigurační postupy
f) dokumentaci zahrnující testy zranitelností a soulad s bezpečnostními požadavky Asseco CEIT, a.s.
g) dokumentaci pro zajištění kontinuity provozu a obnovy po havárii.

V případě vývoje řešení se dodavatel zavazuje:

a. Dodržovat a implementovat prověřené postupy pro bezpečný vývoj softwaru.
b. Je-li předání zdrojového kódu k řešení součástí plnění podle smlouvy, bude umožněn audit vykonávaného nebo provedeného plnění, a to zejména s cílem ověřit, zda se postupovalo podle plnění v souladu se smlouvou.
c. Zajistit, že plnění bude obsahovat pouze ty součásti, které jsou objektivně potřebné pro řádné provozování řešení a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že řešení nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).
d. Pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Asseco CEIT, a.s.
e. Zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých testovacích dat Asseco CEIT, a.s.
f. Zajistit, že v produkčním prostředí Asseco CEIT, a.s. bude dodán pouze předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další potřebné údaje k provozování předmětu plnění
g. Zajistit, že v rámci poskytovaného plnění bude dodáváno řešení v souladu s doporučeními standardů informační bezpečnosti.
h. Poskytnout objednateli potřebnou součinnost v případě, že objednatel vyžaduje/realizuje provedení bezpečnostních testů souvisejících s předmětem plnění. V případě, že objednatel požaduje od dodavatele potvrzení o provedení bezpečnostních testů, bude uvedené dohodnuto samostatnou smluvní dohodou.
i. Předat zdrojový kód Asseco CEIT, a.s., je-li to uvedeno ve smlouvě, bezpečnou formou se zajištěním jeho integrity.
j. Zajistit řízení verzí zdrojového kódu.
k. Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.
l. Zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí pro řízenou kompilaci těchto zdrojových kódů
m. nevyvíjet, nekompilovat a nešířit v prostředí Asseco CEIT, a.s. programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

7 Monitorování

a) Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům Asseco CEIT, a.s. je nepřetržitě zaznamenávaný, monitorovaný a vyhodnocovaný. Události v systémech jsou Asseco CEIT, a.s. zaznamenávány do logů.
b) Dodavatel je povinen průběžně monitorovat v rámci své IKT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

8 Ochrana médií

a. Uložení chráněných informací Asseco CEIT, a.s. na přenosná média a případný transport médií mimo prostory Asseco CEIT, a.s. podléhá jejímu schválení.
b. V případě ukládání chráněných informací Asseco CEIT, a.s. na přenosná média je dodavatel povinen, v technicky proveditelném rozsahu, ukládat, případně vyžadovat uložení těchto údajů v šifrované podobě a vést evidenci těchto médií.
c. Dodavatel je povinen zajistit likvidaci provozních údajů obsahujících chráněné informace Asseco CEIT, a.s. okamžitě po pominutí účelu jejich zpracování a/nebo uložení. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

9 Kybernetické incidenty

Dodavatel je povinen hlásit veškerá podezření na kybernetické incidenty:

a. odpovědné osobě Asseco CEIT, a.s.
b. ve lhůtě bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události/incidentu.
c. formou e-mailu, telefonicky se zajištěním důkazu hovoru na obou stranách, anebo osobně.
d. s popisem:
    - data a času zjištění incidentu;
    - povahy události;
    - zdroje události;
    - cíle/oběti události;
    - potencionálního vlivu.

10 Zákaznický audit

10.1 Oprávnění k provedení auditu

a. Asseco CEIT, a.s. si vyhrazuje právo provádět audity dodavatele.
b. Asseco CEIT, a.s. s dostatečným předstihem alespoň 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že Asseco CEIT, a.s. se zavazuje postupovat tak, aby nenarušil provozní potřeby dodavatele.
c. Asseco CEIT, a.s. si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.
d. Auditor/inspektor stanoví při zjištění neshod nápravná opatření ke zjištění a datum jejich zavedení. Dodavatel je povinen nápravná opatření realizovat v rozsahu stanoveného opatření a v požadovaném termínu.

e. Dokumentace auditů provedených Asseco CEIT, a.s. je vedena v útvaru odpovědném za provádění auditů. Záznamy týkající se určitého auditu jsou vždy označovány stejným identifikátorem. Jednotlivé záznamy auditů tvoří:
   - plán auditu;
   - oznámení o auditu;
   - dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
   - zpráva z auditu;
   - písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisejí s auditem (pokud je nezbytné pro dokumentování nálezů);
   - záznam o zjištění (nápravných opatřeních a následné kontrole).

f. Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění:
   - dodavatel navrhne na základě zjištění uvedených v závěrečné auditorské zprávě návrh opatření a termíny řešení a předá jejich seznam Asseco CEIT, a.s. k odsouhlasení;
   - Asseco CEIT, a.s. potvrdí souhlas s navrhovanými opatřeními.

10.2 Nápravná opatření

a. Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření.
b. Zprávu o realizovaných opatřeních dodavatel oznamuje a předává Asseco CEIT, a.s.

11 Ochrana majetku proti neautorizovaným činnostem

Dodavatel na majetek Asseco CEIT, a. s. neinstaluje a nepoužívá nástroje, které nejsou součástí předmětu plnění.

12 Podmínky ukončení smlouvy

a. V případě ukončení smluvního vztahu musí být ukončeny všechny přístupy dodavatele a jeho zaměstnanců k majetku Asseco CEIT, a.s. (VPN, systémy, informace) nejpozději ke dni ukončení smluvního vztahu.
b. Pokud byl zaměstnancům dodavatele poskytnut majetek Asseco CEIT, a.s., musí být tento majetek vrácen nejpozději ke dni ukončení smluvního vztahu.
c. Pokud zhotovitelům byla poskytnut informační majetek (data) Asseco CEIT, a.s., musí být nejpozději ke dni ukončení smluvního vztahu vrácen a beze zbytku smazán, bez možnosti obnovení, ze všech systémů a nosičů dodavatele.
d. V případě předčasného ukončení smluvního vztahu jiným způsobem než splněním závazku (např. výpovědí, odstoupením od smlouvy, dohodou o ukončení smlouvy apod.), mohou být přístupy

dodavatele, je-li to nutné, ze strany Asseco CEIT, a.s. ukončeny před uplynutím doby trvání smluvního vztahu.