PRAVIDLA CHOVÁNÍ TŘETÍCH STRAN
IT BEZPEČNOST

Dodavatel musí při dodávce Předmětu plnění skupině Veolia dodržovat níže uvedená pravidla.

1. OBECNÁ PRAVIDLA

1.1 Předmět plnění nesmí být zatížen žádnými faktickými ani právními vadami a musí odpovídat všem technickým požadavkům a technickým a bezpečnostním normám pro daný druh plnění, a to jak normám závazným, tak i doporučujícím.

1.2 Předmět plnění musí být schopen podávat trvale standardní výkon v souladu s vlastnostmi a kvalitou stanovenými ve Smlouvě a plně vyhovovat účelu, pro který byl poptán Společností.

1.3 Pracovníci Dodavatele mohou přistupovat k Informačnímu systému Veolia výhradně prostřednictvím autentizačních údajů přidělených Společností.

1.4 Dodavatel se zavazuje dodržovat bezpečnostní pravidla Společnosti (schválení a evidence vstupu, fyzická bezpečnost, požární a bezpečnostní předpisy) v prostorech Společností.

1.5 Dodavatel se zavazuje nakládat s veškerými daty a údaji ke kterým se dostane v IS Veolia přísně důvěrně, nekopírovat je, neumožnit zpřístupnění třetí osobě.

2. BEZPEČNOST KOMUNIKACE

Dodavatel musí chránit Informační systém a Informační aktiva skupiny Veolia a zabránit dle svých nejlepších odborných schopností jejich poškození, zneužití nebo odcizení. V případě ztráty, nebo odcizení HW, SW, nebo dat skupiny Veolia nahlásit tuto skutečnost Oddělení IT Veolia nejpozději do 24 hodin od zjištění, a to i v případě podezření na odcizení (zkopírování) dat, nebo neoprávněného přístupu.

2.1 Pracovní stanice, notebooky

Při práci na Počítači připojeném do Informačního systému VEOLIA musí Dodavatel dodržovat tyto základní zásady:

a) umožnit přístup jen proškolenému pracovníkovi Dodavatele,

b) chránit výpočetní techniku skupiny Veolia,

c) po ukončení práce v Informačním systému VEOLIA provést neprodleně odhlášení tak, aby se zamezilo zneužití jeho přístupových práv.

V případě práce dodavatele v prostorách VEOLIA nebo v jím využívaných prostorách v datových centrech musí dodavatel dále dodržovat tyto zásady:

d) nepřipojovat vlastní Počítač,

e) v blízkosti výpočetní techniky nejíst, nepít a nekouřit.

2.2 Využívání počítačové sítě a internetu

Dodavatel se smí připojovat do Informačního systému Veolia pouze za účelem plnění Předmětu plnění. Dodavatel bere na vědomí a souhlasí s tím, že přístup do Informačního systému Veolia a na internet je v rámci skupiny Veolia filtrován a monitorován.

Dodavatel je oprávněn přistupovat pouze do částí Informačního systému Veolia, které jsou nutné pro Předmět plnění, a na které mu byly pracovníkem oddělení IT přiděleny přístupová oprávnění.

Přístup Dodavatele do IS skupiny Veolia:

a) Vzdálený přístup Dodavatele může být povolen pouze do vývojového a testovacího prostředí za podmínek dohodnutých s oddělením IT skupiny Veolia. Výjimky může povolit pouze Manažer bezpečnosti informací Veolia CZ/SK. Přístup do produkčního prostředí může být s ohledem na citlivost informací monitorován.

b) Lokální přístup Dodavatele do provozního prostředí bude povolen pouze v odůvodněných případech. Tento přístup musí probíhat ve zvláštním režimu dohledu ze strany oddělení IT Veolia.

2.3 Správa serverů a IS

Při práci na serverech IS Veolia musí být splněny následující zásady:

a) Server svěřený Dodavateli do správy musí Dodavatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a konzistence dat.

b) Dodavatel nesmí měnit jakákoliv oprávnění na serveru nebo IS bez písemného souhlasu oddělení IT Veolia.

c) Dodavatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez písemného souhlasu oddělení IT skupiny Veolia.

d) Dodavatel musí zajistit periodickou bezpečnostní aktualizaci operačního systému a aplikačních částí serverů. Bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě skupiny Veolia musí aplikovat neprodleně po jejich vydání.

e) Dodavatel je povinen provádět analýzu systémových a bezpečnostních logů, monitoring a na vyžádání předávat odpovědné osobě definované ve smlouvě písemné zprávy obsahující údaje z analýz sledování a měření běhu IS a zároveň závěry a doporučení s výhledem na další období.

f) Dodavatel je povinen udržovat aktuální dokumentaci k provozovaným systémům, kterou po každé aktualizaci předá oddělení IT skupiny Veolia.

2.4 Bezpečnostní incidenty

a) Dodavatel musí vyvinout maximální úsilí pro odvrácení vzniku bezpečnostních hrozeb pro Informační systém Veolia.

b) Dodavatel musí zajistit maximální součinnost při analýze bezpečnostního incidentu Společností a implementovat nápravná opatření stanovená Společností.

c) V případě podezření či potvrzení vzniku bezpečnostní hrozby pro IS Veolia je Dodavatel povinen neprodleně písemně (emailem) informovat o této skutečnosti zodpovědnou osobu Společnosti či IT oddělení Veolia.

3. POŽADAVKY NA DODÁVANÉ APLIKACE A INFORMAČNÍ SYSTÉMY

3.1. Aplikace

a) Aplikace musí být vytvářeny tak, aby znemožnily přístup bez zadání hesla (aplikace může pro přihlášení využít SSO - využití přihlašovacích údajů z operačního systému případně browseru, které není nutné do aplikace zadávat).

b) Uživatel aplikace musí být nucen si heslo pravidelně měnit.

c) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po deseti neúspěšných pokusech o přihlášení musí být další zadávání dočasně ochromeno nebo spojení rozpojeno.

d) Pokud je při přihlašování do aplikace některá část chybná, nesmí být uživateli poskytnuta informace, ve kterém z údajů je chyba.

e) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností autora aplikace vynutit si změnu tohoto inicializačního hesla.

f) Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor (přihlašovací jméno) tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti.

g) Dodavatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.

h) Systém správy hesel musí být podpořen efektivním a interaktivním vybavením, které prosazuje kvalitu hesel.

i) Hesla musejí být ukládána v zašifrované podobě, pomocí nereverzibilního způsobu šifrování. Nereverzibilní algoritmus šifrování musí využívat kombinaci globální soli a soli specifické pro uživatele, za účelem zablokování většiny slovníkových útoků.

j) Hesla nesmějí být na síti přenášena v nešifrované podobě.

3.2. Monitorování používání systému a přístupů k systému

V informačních systémech musí být pořizovány auditní záznamy obsahující:

a) Identifikaci uživatele;

b) Datum a čas přihlášení a odhlášení;

c) Identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);

d) Záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích;

e) Záznamy musí být možné vzdáleně číst a následně zpracovávat nebo je systém musí automaticky odesílat na vzdálený syslog server.

3.3. Řízení přístupu k informačním systémům

a) Před umožněním přístupu musí být každý uživatel identifikován a autentizován;

b) Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit;

c) Po určitém množství neúspěšných autentizačních pokusů (doporučeno 10) se musí ukončit přihlašovací procedura;

d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informaci o tom, která část autentizace je chybná;

e) Pro každého uživatele systému musí být možné identifikovat, jaká má přístupová práva;

f) Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.);

g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

3.4. Bezpečnost dat

Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V aplikacích se musí evidovat identifikátor uživatele nebo procesu, který změny nebo pořízení provedl.

Pro kontrolu dat musí Dodavatel aplikovat opatření:

- vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...);
- kontrola vnitřního zpracování dat;
- kontrola oprávněnosti běhu programů;
- kontrola integrity dat;
- kontrola obsahu generovaných dat.

Pokud zástupce Společnosti usoudí, že vytvářená aplikace by měla podporovat kryptografii, je nezbytné, aby byly podporovány mezinárodně uznávané standardy a dodrženy právní předpisy České republiky.

3.5. Požadavky na vývoj SW

Vývoj software musí probíhat:

a) Legálním softwarem;

b) Autorská a licenční ujednání musí být smluvně řešena před samotným vývojem.

c) Na testovacím prostředí odděleném od prostředí produkčního;

d) Na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat;

e) Hromadné zpracování dat, nebo jejich výstupy musí být v souladu s platnými bezpečnostními pokyny a směrnicemi skupiny Veolia.

f) Migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení.

4. PŘEDÁNÍ PŘEDMĚTU PLNĚNÍ

4.1. Dodávka software

Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Pokud není stanoveno ve smlouvě jinak, je Dodavatel povinen SW dodat se zdrojovými kódy.

U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice. Pracuje-li počítačový program nebo aplikace, s daty, musí být specifikováno s jakými daty a musí být provedena jejich kategorizace. Obsahuje-li aplikace hromadné výstupy dat, musí se implementovat platné směrnice pro bezpečnost a práci s daty skupiny Veolia.

4.2. Dodávka HW

O každé dodávce Předmětu plnění musí existovat kromě účetních dokladů i předávací protokol podepsaný dodavatelem a odběratelem. Způsob předání závisí na konkrétním HW a na smlouvě s dodavatelem.

4.3. Dodávka služeb

Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.

Dodavatel zajistí monitorování služby tak, aby bylo možné porovnání jejích parametrů, rozsahu a kvality stanovených Smlouvou.

4.4. Dokumentace

Nedílnou součástí dodávky Předmětu plnění je projektová a bezpečnostní dokumentace Předmětu plnění. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s Dodavatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v případě, že ji Dodavatel ve lhůtě stanovené Společností neopraví, důvodem k odstoupení od Smlouvy.

Pokud má být měněn Předmět plnění, musí Dodavatel aktualizovat dokumentaci.

4.5. Akceptace

Každý dodávaný prvek Předmětu plnění musí být plně a široce Dodavatelem otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika (penetrační test, práce s daty).

Každý prvek Předmětu plnění je předán až podpisem písemného předávacího protokolu oprávněnými zástupci smluvních stran.

5. FYZICKÁ BEZPEČNOST

Na pracovištích skupiny VEOLIA není dovolen pohyb cizích osob bez doprovodu pracovníka skupiny VEOLIA a cizí osoba nesmí být zanechána bez dozoru v neveřejné oblasti.

6. POSKYTOVÁNÍ INFORMACÍ TŘETÍM STRANÁM

Dodavatel je povinen dodržovat mlčenlivost o důvěrných informacích skupiny VEOLIA, které se dozvěděl při dodávce Předmětu plnění, a to i v následujících čtyřech letech po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací skupiny VEOLIA se rozumí informace obchodní, technická či jiná, která je konkurenčně významná a není v obchodních kruzích běžně dostupná.

Dodavatel může šířit informace o Předmětu plnění či o spolupráci se Skupinou Veolia (web, medializace Dodavatele, publikace, tisk apod.) jen s předchozím písemným souhlasem Společnosti.

7. PORUŠENÍ PRAVIDEL

Porušení těchto pravidel představuje porušení smlouvy. Pokud Dodavatel poruší tato pravidla hrubým způsobem nebo opakovaně (třikrát v průběhu jednoho měsíce), je společnost skupiny VEOLIA oprávněna odstoupit od smlouvy s Dodavatelem.

Účinnost od 5.4.2016