Vodovody a kanalizace
Pardubice, a.s.
Teplého 2014
530 02 Pardubice

Příloha číslo 3. - Pravidla chování dodavatelů v oblasti bezpečnosti informací.

Společnost Vodovody a kanalizace Pardubice, a.s. (dále jen „Organizace“) od svých dodavatelů (dále jen „Dodavatel“) vyžaduje dodržování těchto pravidel chování v souladu s Politikou bezpečnosti informací Organizace.
Dodavatel bere na vědomí, že Organizace je provozovatelem informačních systémů základní služby v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.
Dodavatel musí při plnění smluvního vztahu (dále jen „Předmět plnění“) pro Organizaci 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, technickým a bezpečnostním normám pro daný druh Předmětu plnění, a to jak normám závazným, tak i doporučujícím.

1.2 Zaměstnanci Dodavatele mohou přistupovat k informačním a komunikačním prostředkům (ICT prostředky) Organizace výhradně prostřednictvím autentizačních údajů přidělených Organizací (např. VPN přístup).

1.3 Dodavatel se zavazuje dodržovat bezpečnostní opatření a pravidla Organizace při práci s informacemi a ICT prostředky Organizace.

1.4 Dodavatel se zavazuje nakládat s veškerými daty, informacemi a údaji, ke kterým se dostane v rámci Předmětu plnění takovým způsobem, aby nemohlo dojít k jejich ztrátě, vyzrazení, neoprávněné či neodborné manipulaci. Dále se zavazuje používat tato data pouze k danému účelu a neumožnit jejich zpřístupnění nepovolané osobě.

1.5 Dodavatel se zavazuje dodržovat veškerou platnou legislativu, zejména pak tu v oblasti kybernetické bezpečnosti a ochrany osobních údajů.

2 Bezpečnost komunikace

2.1 V případě ztráty nebo odcizení hardware, software, dat, informací Organizace musí Dodavatel vždy neprodleně nahlásit tuto skutečnost oddělení ICT Organizace, a to i v případě pouhého podezření na neoprávněný přístup a manipulaci s daty.

2.2 Dodavatel hlásí skutečnosti oddělení ICT Organizace vždy na e-mail: jan.klepac@vakpce.cz, jiri.semerad@vakpce.cz, martin.pilar@vakpce.cz a telefonicky na

tel.: +420 606 604 010, záložní +420 724 392 239 (Organizace výslovně vyžaduje duplicitní informaci, tedy telefonem a zároveň i e-mailem).

2.3 **Při práci na zařízení (například: počítači, notebooku, mobilním telefonu**, **SCADA prostředku)** připojeném do sítě a/nebo k informačním systémům Organizace musí Dodavatel dodržovat tyto zásady:

- umožnit přístup jen proškolenému zaměstnanci Dodavatele,
- chránit výpočetní techniku a všechna data Organizace před porušením důvěrnosti, integrity či dostupnosti,
- po ukončení práce v síti a/nebo v informačním systému Organizace provést neprodleně odhlášení uživatele.

2.4 **Při práci na serverech** Organizace musí být splněny následující zásady, které se vztahující i na servisní (provozní) smlouvy (s ohledem na specifikace informačních systémů):

- Zařízení svěřeno Dodavateli do správy musí Dodavatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a integrity dat, pokud není v servisní smlouvě sjednáno jinak.
- Dodavatel nesmí měnit jakákoliv oprávnění na serveru nebo informačním a komunikačním systému bez souhlasu odboru Správy informačního systému, pokud není v servisní smlouvě sjednáno jinak.
- Dodavatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu odboru Správy informačního systému, pokud není v servisní smlouvě sjednáno jinak.
- Pokud je v servisní smlouvě sjednáno, tak Dodavatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě Organizace, musí aplikovat neprodleně po jejich vydání.
- Dodavatel je povinen udržovat aktuální dokumentaci k servisovaným informačním a komunikačním systémům, kterou po každé aktualizaci musí předat oddělení ICT.

2.5 **Při práci v interní sítí** Organizace odpovídají zaměstnanci Dodavatele, kteří mají přidělen přístup do interní sítě Organizace, za své činnosti prováděné v rámci této sítě. Zaměstnanci Dodavatele nesmí, zejména:

- zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě,
- šířit či jinak nakládat se škodlivým malwarem,
- využívat nástroje sloužící k maskování identity,
- provádět bezdůvodné skenování portů či jiných parametrů sítě a síťových zařízení,
- provádět jakoukoliv formou monitorování sítě, které může vést k zachycení dat, pokud není Předmětem plnění smlouvy s Organizace,
- obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, sítě nebo uživatelského účtu,
- provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům,
- užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes síť, internet nebo intranet,

- využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemce, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů),
- předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec Organizace, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

3 Kybernetické bezpečnostní události a incidenty

3.1 Dodavatel musí plnit své povinnost uvedené ve smlouvě, pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy Organizace.

3.2 Dodavatel musí zajistit součinnost uvedenou ve smlouvě, při analýze kybernetických bezpečnostních událostí a incidentů Organizace a následně po dohodě zavádět vhodná nápravná opatření určené Organizace.

3.3 V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém Organizace je Dodavatel povinen neprodleně písemně (e-mailem) či telefonicky (a následně také písemně) informovat o této skutečnosti Manažera kybernetické bezpečnosti Organizace.

4 Požadavky na dodávané informační systémy

4.1 **Požadavky na dodávané informační systémy**

- Informační systém musí být vytvářen tak, aby dostatečně chránil data před porušením důvěrnosti, dostupnosti a integrity.
- Informační systém musí být vytvořen tak, aby byla každá operace uložena v provozním záznamu (logu) s jedinečným identifikátorem uživatele, který tuto operaci vykonal. Musí být zajištěno, aby nemohlo dojít k provádění operací pod cizím identifikátorem uživatele.
- Informační systém musí obsahovat funkcionalitu, kterou lze nastavit vymáhání pravidelné změny hesla uživatele.
- Informační systém musí obsahovat funkcionalitu, kterou lze nastavit počet neúspěšných pokusí o přihlášení na šest pokusů, pak musí být další zadávání dočasně zablokováno nebo spojení rozpojeno.
- V případě, že je povolen přístup do informačního systému, v němž určuje vstupní heslo administrátor, je povinností autora informačního systému vynutit si změnu tohoto inicializačního hesla.
- Dodavatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.
- Dodavatel musí zajistit integraci informačního systému na IDM Organizace, pokud je to technicky možné.

4.2 **V informačních systémech musí být pořizovány auditní záznamy obsahující alespoň:**

- identifikaci uživatele;

- datum a čas přihlášení a odhlášení;
- identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);
- záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích;
- záznamy musí být možné vzdáleně číst a následně zpracovávat nebo je systém musí automaticky odesílat na vzdálený SOC Organizace.

4.3 **Řízení přístupu k informačním systémům**

- Před umožněním přístupu musí být každý uživatel identifikován a autentizován.
- Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.
- Po určitém množství neúspěšných autentizačních pokusů (doporučeno 6) se musí ukončit přihlašovací proces.
- V případě neúspěšné autentizace nesmí informační systém poskytnout uživateli informaci o tom, která část autentizace je chybná.
- Administrátor informačního systému musí mít možnost identifikovat přidělená přístupová práva pro každého uživatele informačního systému.
- Pro každý informační systém musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto informačnímu systému s rozlišením druhu přístupových práv (čtení, úprava atd.).
- Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

4.4 Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V informačních systémech se musí evidovat identifikátor uživatele, který změny 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.

4.5 Vývoj software musí probíhat:

- legálním softwarem,
- autorská a licenční ujednání musí být smluvně řešena před samotným vývojem,
- na testovacím prostředí odděleném od prostředí produkčního,
- na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat,
- migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém či testovacím prostředí.

Vodovody a kanalizace
Pardubice, a.s.
Teplého 2014
530 02 Pardubice

5 Předání plnění

Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.

5.1 Dodávka software

- Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Pokud není stanoveno ve smlouvě jinak, je Dodavatel povinen software 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.

5.2 Dodávka hardware

- Ke každé dodávce musí existovat kromě účetních dokladů I předávací protokol podepsaný Dodavatelem a Organizace. Způsob předání závisí na konkrétním hardware a na smlouvě s Dodavatelem.

5.3 Dodávka služeb

- Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.
- Dodavatel zajistí monitorování služby tak, aby bylo možné porovnání jejich parametrů, rozsahu a kvality stanovených Smlouvou.

5.4 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 Organizace neopraví, důvodem k odstoupení od Smlouvy.
- Pokud má být měněn Předmět plnění, musí Dodavatel aktualizovat dokumentaci.

5.5 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.

Vodovody a kanalizace
Pardubice, a.s.
Teplého 2014
530 02 Pardubice

6 Fyzická bezpečnost

6.1 Na neveřejných pracovištích a prostorách Organizace (např. datové centrum) není dovolen pohyb cizích osob bez dozoru zaměstnance Organizace.

6.2 Zaměstnanci Dodavatele mohou fyzicky přistupovat k ICT prostředkům Organizace pouze v doprovodu oprávněné osoby Organizace.

6.3 V případě práce Dodavatele v prostorách Organizace nebo v jím využívaných prostorách v datových centrech musí Dodavatel dále dodržovat tyto zásady:

- připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby Organizace,
- v blízkosti ICT prostředků nejíst, nepít a nekouřit.

6.4 Dodavatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace Organizace.

7 Poskytování informací třetím stranám

7.1 Dodavatel je povinen dodržovat mlčenlivost o důvěrných informacích Organizace, které se dozvěděl při dodávce Předmětu plnění, a to i po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací Organizace se rozumí informace obchodní, technická, osobní údaje, zdravotnická dokumentace či jiná, která je významná pro Organizace a/nebo je konkurenčně významná a není v obchodních kruzích běžně dostupná.

7.2 Pokud Dodavatel přijde do styku s osobními údaji, musí se řídit platnou legislativou na ochranu osobních údajů, především týkající se zpracování a předávání. Je-li zpracovatelem osobních údajů, podepíše zpracovatelskou smlouvu.

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

8 Bezpečnostní nástroje

8.1 Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Organizace. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

- Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
- Realizovat přístup z mobilního zařízení do prostředí Organizace pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.

- Připojovat do prostředí Organizace pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a o jejich připojení bylo schváleno oprávněnou osobou ve věcech technických na straně Organizace určených ve smlouvě.
- Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Dodavatele.
- Na aktiva Organizace neinstalovat a nepoužívat v prostředí Organizace tyto typy nástrojů, pokud nejsou součástí předmětu plnění:
  - Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
  - Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
  - Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
  - Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
  - Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
- Připojovat do prostředí Organizace pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.
- Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.
- Na vyžádání poskytnout Organizaci report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.
- Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
- Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
- Veškeré neveřejné informace poskytnuté Organizací chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

8.2 Dodavatel bere na vědomí, že v případě, kdy technické spojení Organizace s Dodavatelem narušuje chod služeb Organizace, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud smlouva nestanoví jinak.
8.3 Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Organizace jsou monitorovány a vyhodnocovány v rozsahu předmětu plnění a v souladu s interními dokumenty Organizace, se kterými byl Dodavatel seznámen.

Vodovody a kanalizace
Pardubice, a.s.
Teplého 2014
530 02 Pardubice

9 Porušení pravidel

9.1 Porušení těchto pravidel představuje porušení Předmětu plnění. Pokud Dodavatel poruší tato pravidla hrubým způsobem nebo opakovaně, je Organizace oprávněna odstoupit od smluvního vztahu s Dodavatelem.