



KUJCP01BRDQ2

Dodatek č. 2
ke Smlouvě o zajištění funkce manažera
kybernetické bezpečnosti SON/OINF/021/18
ze dne 12. 11. 2018

dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník

Smluvní strany:

Jihočeský kraj

Sídlo: U Zimního stadionu 1952/2, 370 76 České Budějovice

Zastoupený: Ing. Petrem Vobejdou, vedoucím odboru informatiky

IČO: 70890650

DIČ: CZ70890650

Bankovní spojení: ČSOB, a.s.

Číslo účtu: 199783072/0300

Objednatel je plátcem DPH

(dále jen „Objednatel“)

a

Ing. Martin Havel, MBA

Sídlo: Velešovická 20, 683 01 Rousínov

IČO: 66565090

DIČ: CZ7101084364

Bankovní spojení: Česká spořitelna a.s.

Číslo účtu: 1153773033/0800

Poskytovatel je plátcem DPH

(dále jen „Poskytovatel“)

Čl. I. Předmět dodatku

Čl. V. Závěrečná ustanovení (Smlouvy o zajištění funkce manažera kybernetické bezpečnosti) se doplňuje následovně:

5.4 Poskytovatel se zavazuje postupovat podle přílohy č. 1 této smlouvy – Bezpečnostní pravidla pro dodavatele.

Čl. II. Závěrečná ustanovení

2.1 Tento dodatek nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění v registru smluv.

2.2 Tento dodatek je vyhotoven ve dvou stejnopisech, z nichž po jednom obdrží každá ze smluvních stran.

Příloha č. 1 – Bezpečnostní pravidla pro dodavatele.

V Českých Budějovicích dne **31-10-2019**

V Rousínově dne **25.10.2019**

Za Objednatele:
Ing. Petr Vobejda

JIHOČESKÝ KRAJ
KRAJSKÝ ÚŘAD
odbor informatiky

U Zimního stadionu 1952/2
370 76 České Budějovice (2)

Za Poskytovatele:
Ing. Martin Havel, MBA

Bezpečnostní pravidla pro Dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva KÚ JK, ke kterým mají přístup Dodavatelé.

A.1 Základní odpovědnosti Dodavatele

Dodavatel řešení:

- a. Je povinen dodržovat požadavky na bezpečnost informací v souladu s platnými zákony ČR.
- b. Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KÚ JK, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.
- c. Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.
- d. Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s úřadem.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarům IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

A.2 Ochrana Aktiv

Dodavatel se před vlastním **přístupem** k datům a informacím KÚ JK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KÚ JK (prioritně ve smlouvě, prohlášením Dodavatele, formulářem,...) zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

A.3 Přístup k ICT/IS

Přihlášení Dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

A.4 Ochrana před škodlivým softwarem

Dodavatel je povinen:

- a. Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK.
- b. Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury Dodavatele.
- c. Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.
- d. Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

A.5 Řízení bezpečnostních rizik

Dodavatel je povinen zajistit, že:

- a. Hesla pracovníků Dodavatele nebudou zaznamenávána v otevřené podobě.

- b. Vzájemnou spolupráci a komunikaci mezi Dodavatelem a KÚ JK při řešení ICT bezpečnostní rizik

A.6 Hlášení

Dodavatel je povinen KÚ JK hlásit:

1. nestandardní situace při práci v ICT/IS;
2. bezpečnostní události nad ICT/IS;
3. bezpečnostní slabiny v ICT/IS Objednatele.

A.7 Kontrola a audit Dodavatele

KÚ JK má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostních pravidel Objednatele či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele a to minimálně 1x za 12 měsíců.

A.8 Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti, který má právo výjimku udělit.

Schváleno: Bezpečnostní komise - Výbor pro řízení kybernetické bezpečnosti

Datum: 26. 8. 2019

Platné od: 26. 8. 2019