|  |  |  |  |
| --- | --- | --- | --- |
| Příloha | č. 2 | Smlouvy | SML/0434/24 |

PRAVIDLA kybernetické bezpečnosti PRO DODAVATELE

Obsah

[1 Preambule 2](#_Toc184706467)

[2 Obecné požadavky bezpečnosti informací 2](#_Toc184706468)

[3 Personální bezpečnost 3](#_Toc184706469)

[4 Fyzická ochrana a bezpečnost prostředí 4](#_Toc184706470)

[5 Oprávnění užívat data a autorství programového kódu 4](#_Toc184706471)

[6 Kontrola a audit dodavatele (pravidla zákaznisckého auditu) 4](#_Toc184706472)

[7 Řetězení dodavatelů 4](#_Toc184706473)

[8 Řízení přístupu 5](#_Toc184706474)

[9 Řízení změn a kontinuita činností 5](#_Toc184706475)

[10 Monitorování činností 6](#_Toc184706476)

[11 Zvládání kybernetických bezpečnostních incidentů 6](#_Toc184706477)

[12 Ochrana důvěrnosti informací 6](#_Toc184706478)

[13 Informační povinnosti Dodavatele 6](#_Toc184706479)

[14 Povinnosti při ukončení Smlouvy 6](#_Toc184706480)

[15 Specifikace podmínek pro předání dat, údajů a informací 7](#_Toc184706481)

[16 Pravidla pro likvidaci dat 7](#_Toc184706482)

[17 Sankce a důsledky porušení povinnosti 7](#_Toc184706483)

# Preambule

Společnost Brněnské vodárny a kanalizace, a.s. (dále „BVK“ nebo „Objednatel“) je správcem informačního systému základní služby ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),

**Tento dokument je nedílnou součástí smlouvy s významným dodavatelem (dále „Dodavatel“) dle zákona č. 181/2014 Sb.,** **o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),** v platném znění (dále jen „ZoKB“). V souladu s ustanovením § 4 odst. 4a § 8 odst. 1 písm. a) a f) ZoKB a ve spojení s přílohou č. 7 vyhl. č. 82/2018 Sb. (dále jen „VoKB“) jsou dále definována závazná bezpečnostní opatření zohledňující požadavky systému řízení bezpečnosti informací, která se vztahují na významné dodavatele, kteří pro Brněnské vodárny a kanalizace a.s. (dále jen „BVK“) výhradně či jako součást předmětu plnění dodávají, vyvíjí, implementují software či hardware (dále také jen „SW“ či „HW“), a/nebo provádějí servis SW či HW, a/nebo kteří v souvislosti s plněním pro BVK přistupují do informačního systému BVK, který byl určen informačním systémem základní služby (dále také „ISZS“) v souladu se ZoKB, a/nebo kteří v rámci poskytovaného plnění pro společnost BVK zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo uchovávají informace, data a/nebo provozní údaje BVK.

Účelem tohoto dokumentu je dosažení stanovené úrovně bezpečnosti informací v souladu s požadavky ZoKB, VoKB a dokumentace systému řízení bezpečnosti informací společnosti BVK.

Dodavatel (v textu Smlouvy označen jako „zhotovitel“) podpisem Smlouvy prohlašuje, že si je vědom všech povinností, které je povinen z hlediska zachování bezpečnosti informací v BVK dodržovat. Je-li nezbytné omezit, ohrozit nebo přerušit, důvěrnost, dostupnost či integritu informací a dat, může tak dodavatel učinit pouze po předchozím souhlasu BVK a jen v rozsahu BVK předem odsouhlaseném.

Práva a povinnosti Dodavatele stanovená tímto dokumentem se považují za bezpečnostní opatření BVK.

„Dodavatelem“ se pro účely tohoto dokumentu rozumí významný dodavatel dle ZoKB, kterým je každá osoba, poskytující BVK jakékoliv plnění související s ISZS na základě smlouvy, nebo objednávky.

„Smlouvou“ se pro účely tohoto dokumentu rozumí smlouva uzavřená mezi BVK a Dodavatelem HW nebo SW souvisejícího s ISZS..

„Aktivem“ se pro účely tohoto dokumentu rozumí primární aktivum, nebo podpůrné aktivum ve smyslu § 2 písm. f), nebo g) VoKB.

Není-li dále uvedeno jinak, jsou pojmy užívané v tomto dokumentu pojmy ve smyslu ZoKB, VoKB, nebo dokumentace systému řízení bezpečnosti informací ve společnosti BVK.

# Obecné požadavky bezpečnosti informací

Dodavatel je při poskytování plnění pro BVK povinen plnit následující povinnosti.

* postupovat v souladu s platnými právními předpisy, s důrazem na ZoKB a VoKB a vyvarovat se jakékoliv činnosti, která by mohla být označena za porušení právních předpisů a vnitřních předpisů BVK, se kterými byl prokazatelně seznámen.
* zachovat bezpečnost informací a dat obsažených v ISZS, nebo v jiných informačních systémech, které jsou plněním Smlouvy dotčeny, a to zejména z pohledu důvěrnosti, dostupnosti a integrity.
* informovat písemně BVK o způsobu řízení rizik na straně Dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy, a to do 15 pracovních dnů od nabytí účinnosti Smlouvy.
* jmenovat nejpozději do 3 pracovních dnů po nabytí účinnosti Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních opatření a související komunikace mezi smluvními stranami, není-li ve Smlouvě stanoveno jinak.
* zajistit, aby kontaktní osoba Dodavatele nejpozději do 30 dnů od nabytí účinnosti Smlouvy potvrdila písemně BVK, že všechny osoby podílející se na poskytování plnění Smlouvy za stranu dodavatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s tímto dokumentem.
* zavést opatření pro ochranu zálohy dat vztahujících se k plnění Smlouvy a pravidelně testovat funkčnost těchto záloh.
* garantovat schopnost podílet se na rekonstrukci funkcionality aktiva do stavu požadovaného dle Smlouvy.
* realizovat bezpečnostní opatření pro ochranu dat souvisejících s plněním předmětu Smlouvy.
* upozornit Objednatele na jakoukoliv vydanou softwarovou aktualizaci (upgrade, update, service pack vč. bezpečnostních patchů apod.) bez zbytečného odkladu od okamžiku vydání aktualizace
* podílet se na koordinaci provedení aktualizace software u Objednatele tak, aby k ní došlo v co nejbližší možné době a zároveň proces aktualizace co nejméně zasáhl do běžných provozních činností Objednatele (minimalizace doby trvání servisního okna, vhodná volba dne a času k provedení aktualizace apod.).
* upozornit Objednatele na jakoukoliv zjištěnou zranitelnost systému, bez zbytečného odkladu od okamžiku zjištění zranitelnosti.
* poskytovat BVK v termínech stanovených BVK, resp. bez zbytečného odkladu, požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či po jeho předání.
* dodat podklady pro zpracování systémové a provozní bezpečnostní dokumentace BVK, která bude obsahovat minimálně následující:
* provozní a bezpečnostní dokumentace,
* popis principů autentizace, autorizace a vytváření auditních stop,
* popis principů instalace a konfigurace;
* popis nezbytných bezpečnostních konfigurací,
* popis principů zálohování a archivace,
* plány kontinuity činností a havarijní plány.
* chránit veškeré informace vyžadující vyšší míru ochrany, zejména přístupová oprávnění, hesla, identifikační a jiné kritické údaje, poskytnuté BVK při poskytování plnění proti neautorizovanému přístupu; certifikáty a přístupová oprávnění uchovávat v šifrovaném tvaru, pokud nebude mezi smluvními stranami pro konkrétní případ dohodnuto jinak.
* zajistit, aby v produkčním prostředí systému ISZS byl obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému ISZS.
* provést kontrolu souladu daného SW s bezpečnostními opatřeními BVK před spuštěním SW v produkčním prostředí daného ISZS ,v případě zjištění nesouladu zajistit bez zbytečného odkladu soulad dodávaného SW s bezpečnostními opatřeními, pokud byl s takovými opatřeními seznámen.
* nést odpovědnost za to, že SW implementované do ISZS budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace.

# Personální bezpečnost

Pokud Dodavatel využívá při poskytování plnění BVK poddodavatele, zavazuje se zajistit dodržování veškerých bezpečnostních opatření stanovených BVK ve smluvních vztazích se svými poddodavateli a tuto skutečnost doložit BVK na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem, případně předložením čestného prohlášení o řádném naplňování této povinnosti.

Dodavatel a jeho případní poddodavatelé jsou povinni interně (v rámci své organizace) realizovat tato opatření:

* mít stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah;
* realizovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
* zajistit realizaci teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;
* v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
* v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pro osoby zastávající bezpečnostní role pravidelná odborná školení, zohledňující aktuální potřeby v oblasti kybernetické bezpečnosti;
* v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
* vést o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly;
* zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
* v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistit předání odpovědností;
* hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;
* určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

# Fyzická ochrana a bezpečnost prostředí

Dodavatel se zavazuje, že:

* na pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k ISZS, který je předmětem plnění dle Smlouvy.
* bude dodržovat režimová opatření (provozní řády) budov a prostor zejména, kde jsou umístěna aktiva ISZS**.**

# Oprávnění užívat data a autorství programového kódu

Dodavatel je při poskytování plnění pro Objednatele:

* oprávněn užívat data předaná Dodavateli Objednatelem za účelem plnění předmětu Smlouvy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy a zavazuje se nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a VoKB.
* povinen zajistit, aby při plnění Smlouvy dodržel podmínky stanovené zák. č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

# Kontrola a audit dodavatele (pravidla zákaznického auditu)

Dodavatel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti uvedené v tomto dokumentu a v ZoKB a VoKB a umožnit Objednateli provedení auditů prováděných Objednatelem či pověřeným auditorem.

Objednatel je povinen písmeně oznámit Dodavateli provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu.

Dodavatel je povinen:

* poskytnout Objednateli nezbytnou součinnost a zpřístupnit veškerou potřebnou dokumentaci technických a organizačních opatření.
* umožnit kontrolu nebo audit u Dodavatele nebo jeho poddodavatele.
* pravidelně provádět kontrolu zavedených bezpečnostních opatření a hodnocení rizik.
* podniknout nezbytná opatření, která povedou k nápravě neuspokojivých výsledků hodnocení Dodavatele, nebo výsledků provedeného zákaznického auditu.

# Řetězení dodavatelů

Dodavatel není oprávněn zapojit do plnění Smlouvy žádného dalšího poddodavatele bez předchozího schválení Objednatele.

Dodavatel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů.

Pokud Dodavatel využívá za účelem plnění předmětu Smlouvy poddodavatele, musí být tomuto poddodavateli uloženy na základě Smlouvy s Dodavatelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná tímto dokumentem mezi Objednatelem a Dodavatelem.

Dodavatel se zavazuje předložit Objednateli, na základě jeho písemného vyzvání, příslušnou smlouvu s poddodavatelem.

Dodavatel má povinnost zajistit, aby poddodavatel plnil  požadavky, které Objednatel ukládá na základě tohoto dokumentu Dodavateli.

# Řízení přístupu

Přístup k ISZS je možné povolit pouze po evidenci osoby zastupující dodavatele v registru identit BVK nebo obdobném systému BVK, a to na základě požadavku dodavatele na přístup.

Přidělení oprávnění zaměstnancům Dodavatele musí být řízeno principem nezbytného minima a není nárokové.

Dodavatel se zavazuje, že:

* zajistí, aby udělený přístup nebyl sdílen více zaměstnanci Dodavatele ani poddodavatele.
* nepřipojí koncové zařízení do sítě BVK bez předchozího schválení připojení určenou osobu na straně BVK
* zajistí, aby všechny jeho informační systémy, které se připojují do síťové infrastruktury BVK byly chráněny vhodným způsobem proti malware.
* zajistí, aby osoby podílející se na poskytování plnění BVK, které přistupují do interní sítě a/nebo ISZS BVK chránily autentizační prostředky a údaje k ISZS BVK.

Dodavatel bere na vědomí, že:

* v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu).
* postup při zvládání kybernetické bezpečnostní události či jiný důsledek porušení bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany BVK.

# Řízení změn a kontinuita činností

BVK u významných změn dokumentuje jejich řízení, provádí analýzu rizik, přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci, zajistí testování ISZS a zajistí možnost navrácení do původního stavu.

BVK má povinnost informovat Dodavatele o výsledcích řízení změn, které mají dopady na plnění předmětu Smlouvy ze strany dodavatele.

Dodavatel má povinnost:

* přijmout účinná opatření ke snížení nepříznivých dopadů v souladu s výsledky řízení změn.
* poskytnout BVK veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

BVK má oprávnění zapojit Dodavatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Dodavatele do plánu kontinuity činností, který souvisí s ISZS nebo s jeho HW komponentami a souvisejících služeb a/nebo zahrnutí dodavatele do havarijního plánu BVK.

# Monitorování činností

Dodavatel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v  prostředí BVK budou průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na oprávněné zájmy BVK, jakož i s ohledem na obsah Smlouvy a interních dokumentů BVK, se kterými byl dodavatel prokazatelně seznámen.

# Zvládání kybernetických bezpečnostních incidentů

Dodavatel se zavazuje, že:

* při poskytování plnění pro BVK stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny kybernetické bezpečnostní události a incidenty včetně případů porušení zabezpečení osobních údajů neprodleně po jejich detekci BVK.
* se bude podílet na návrhu řešení tak, aby bylo možné zvládat a detekovat kybernetické bezpečnostní události a incidenty a bude se podílet na realizaci opatření pro zvýšení odolnosti informačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom zejména z požadavků stanovených VoKB.
* se bude podílet na provedení analýzy příčin kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a na návrhu opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

# Ochrana důvěrnosti informací

Smluvní strany se zavazují že:

* zachovají mlčenlivost o veškerých informacích a osobních údajích, o nichž se dozvěděly v souvislosti s plněním Smlouvy, a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí stran
* zajistí, aby všechny osoby, oprávněné zpracovávat informace a osobní údaje, o nichž se dozvěděly v souvislosti s plněním Smlouvy, se zavázaly k mlčenlivosti; závazek mlčenlivosti a ochrany důvěrnosti informací zůstává v platnosti i po ukončení Smlouvy.

# Informační povinnosti Dodavatele

Dodavatel má povinnost:

* neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu Smlouvy; součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.
* informovat Objednatele o způsobu řízení rizik a o rizicích souvisejících s plněním předmětu Smlouvy, a to na základě písemné výzvy Objednatele.
* bez zbytečného odkladu informovat Objednatele o významné změně ovládání Dodavatele dle zák. č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví základních aktiv a změně v oprávnění Dodavatele nakládat s aktivy, které jsou využívány k plnění předmětu Smlouvy. v případě, že dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení, je BVK oprávněn odstoupit od Smlouvy.

# Povinnosti při ukončení Smlouvy

Dodavatel se zavazuje:

* poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace při ukončení Smlouvy.
* účastnit se dle pokynů Objednatele jednání s BVK a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, údržbou a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti Smlouvy.,

# Specifikace podmínek pro předání dat, údajů a informací

Veškerá uživatelská a/nebo provozní data ISZS musí být BVK předána bez zbytečného odkladu po doručení žádosti o export, a to v elektronické, strojově čitelné podobě, v otevřeném formátu, jehož využití BVK není zatíženo právy třetích osob a BVK jej může užít bez jakéhokoliv omezení. Součástí předávaných exportovaných dat musí vždy být úplný popis formátu včetně datových typů a vzájemných vazeb v českém jazyce, ledaže by se jednalo o otevřený, standardizovaný formát. Pokud nestanoví BVK jinak, je dodavatel povinen data exportovat v kódování českého jazyka UTF-8. Soulad exportovaných dat s těmito požadavky a jejich úplnost, podléhá akceptaci BVK.

# Pravidla pro likvidaci dat

Dodavatel se zavazuje poskytnout BVK veškerou potřebnou součinnost pro likvidaci nepotřebných dat. Za tím účelem smluvní strany dohodnou lhůty pro provádění likvidace dat, kde stanoví konkrétní rozsah a časové intervaly pro likvidaci dat. Smluvní strany sjednávají, že k likvidaci dat přistoupí po vzájemném odsouhlasení likvidace, podmínky likvidace musí být v souladu přílohou č. 4 VoKB.

# Sankce a důsledky porušení povinnosti

Kromě sankčních ujednání stanovených ve Smlouvě je Objednatel oprávněn odstoupit od smlouvy v případě že:

* Dodavatel nesplní informační povinnost stanovenou mu tímto dokumentem, nebo,
* dojde u Dodavatele k významné změně kontroly nad osobou Dodavatele, nebo,
* dojde u Dodavatele ke změně kontroly nad zásadními Aktivy Dodavatele využívanými k plnění Smlouvy, nebo,
* Dodavatel zapojí do plnění Smlouvy poddodavatele bez písemného souhlasu BVK,

Účinky odstoupení nastávají dnem doručení odstoupení od Smlouvy Dodavateli. Odstoupení nezbavuje dodavatele povinnosti poskytnout součinnost dle ustanovení tohoto dokumentu při ukončení Smlouvy. Sankční ujednání se řídí Smlouvou.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| V Brně dne | 13. 12. 2024 |  | V | Brně | dne | 13. 12. 2024 |
| Za Objednatele |  | Za Dodavatele |
|  |  |  |
| Brněnské vodárny a kanalizace, a.s.Ing. Daniel Struž, MBApředseda představenstva |  | XXX |