STATUTÁRNÍ MĚSTO
KARVINÁ

Bezpečnostní politika informací SMK

Bezpečnostní směrnice pro dodavatele (verze 4)

Schváleno:	28. 05. 2018
Účinnost:	29. 05. 2018
Zpracovatel:	Odbor organizační

Článek 1
Úvodní ustanovení

1.1 Pro účely této směrnice se rozumí:

a) správcem orgán statutárního města Karviné nebo jím zřízená příspěvková organizace, v níž se uplatňuje tato bezpečnostní politika,

b) zpracovatelem subjekt, který má se správcem uzavřenu smlouvu za účelem poskytování dodávek nebo služeb (dále jen „zvláštní smlouva“) a smlouvu o ochraně informací,

c) informacemi veškeré informace, údaje a data, které se zpracovatel doví v přímé i nepřímé souvislosti s plněním předmětu zvláštní smlouvy nebo přístupem zpracovatele k prostředkům pro zpracování informací správce nebo při poskytnutí informací správcem ke zpracování zpracovateli, zejména všechna data, dokumenty, počítačová média a informace všech druhů a v jakékoliv formě, hmotné či nehmotné, které jsou vzájemně poskytovány smluvními stranami písemně nebo ústně, při prezentaci či jinak v souladu se zvláštní smlouvou nebo k nim zpracovatel získal nahodilý přístup; obsahem informací mohou být též osobní údaje podle zvláštního předpisu[1],

d) uživatelem zaměstnanec zpracovatele, jemuž byly zpřístupněny informace nebo prostředky pro zpracování informací správce,

e) prostředky pro zpracování informací jakékoliv analogové nebo digitální zařízení nebo počítačový program, který slouží k pořizování, ukládání, zpracování či likvidaci informací,

f) sjednaným úkonem se rozumí činnost zpracovatele, která spočívá ve zpracování informací nebo provedení změny v prostředcích pro zpracování informací v souvislosti s plnění zvláštní smlouvy,

g) škodlivým kódem počítačový program určený ke vniknutí do počítačového systému, získání neoprávněného přístupu k informacím nebo poškození počítačového systému,

h) bezpečnostní událostí každá událost, která může ohrozit bezpečnost informací, prostředků nebo služeb v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky,

[1] Nařízení Evropského parlamentu a Rady č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/45/ES (obecné nařízení o ochraně osobních údajů).

i) bezpečnostním incidentem narušení bezpečnosti informací, služeb nebo prostředků v důsledku bezpečnostní události,

j) bezpečnostní slabinou zjištěný stav prostředků nebo prostředí, který může způsobit vznik bezpečnostního incidentu.

1.2 Tato směrnice stanovuje povinnosti zpracovatele spojené s přístupem k informacím správce nebo jeho prostředkům pro zpracování informací (dále jen „prostředky“). Je závazná pro všechny zaměstnance zpracovatele, kteří mají přístup k informacím a prostředkům správce. Tito zaměstnanci zpracovatele (dále jen „uživatelé“) mají povinnost seznámit se a dodržovat tuto bezpečnostní směrnici.

Článek 2
Obecná pravidla pro nakládání s informacemi

2.1 Zpracovatel je povinen přijmout a zavést všechna opatření, aby zajistil důvěrnost, dostupnost, integritu a odolnost systémů, služeb a prostředků a byl schopen obnovit dostupnost informací a přístup k nim v případě bezpečnostního incidentu.

2.2 Uživatel musí se všemi informacemi správce, se kterými přijde do styku, zacházet jako s informacemi chráněnými, bez ohledu na jejich skutečné zařazení do stupně klasifikace, která je definována v Celkové bezpečnostní politice. Tato klasifikace se na uživatele dle této bezpečnostní směrnice nevztahuje.

2.3 Uživatel nesmí bez souhlasu správce ukládat jakékoliv informace získané z prostředků správce mimo tyto prostředky.

2.4 Informace, které byly uloženy mimo prostředky správce, musí uživatel po ukončení provádění sjednaného úkonu zničit (skartovat). Skartací informací a dat se rozumí zničení jejich fyzického nosiče nebo smazání z datových úložišť tak, aby je nebylo možné znovu obnovit.

2.5 Uživatel nesmí jakýmkoliv způsobem sdělovat nebo poskytovat jiným osobám jakékoliv informace získané od správce nebo z jeho prostředků.

2.6 Ochrana informací se nevtahuje na informace, které jsou zjevně informacemi veřejnými, a nevztahuje se na ně ochrana dle jiného předpisu[1].

Článek 3
Pravidla pro zpracování osobních údajů

3.1 Zpracovatel je povinen zajistit, aby všichni uživatelé byli zavázáni k mlčenlivosti.

3.2 Uživatelé smí zpracovávat osobní údaje pouze na základě doložených pokynů správce.

3.3 Zpracovatel bez předchozího písemného povolení správce nesmí zapojit do zpracování osobních údajů další subjekt. V případě zapojení dalšího subjektu, je zpracovatel povinen na základě smlouvy mu stanovit povinnosti a odpovědnosti ve stejném rozsahu, jak stanovuje tato bezpečnostní politika zpracovateli.

3.4 Zpracovatel je povinen se správcem spolupracovat při naplňování práv subjektů údajů.

Článek 4
Pravidla pro zálohování dat

4.1 Uživatel je povinen vždy před provedením sjednaného úkonu zajistit bezpečné zálohování dat, která by mohla být při prováděným úkonem dotčena. Záloha dat musí být provedena takovým způsobem, aby umožňovala obnovení stavu před provedením sjednaného úkonu.

4.2 Záložní data nesmí být bez souhlasu správce uložena mimo jeho prostředky. Uživatel musí správce informovat o umístění záložních dat.

4.3 Smazání záložních dat provádí buď správce, nebo uživatel na základě souhlasu správce. Dobu uchování záložních dat určuje správce.

Článek 5
Pravidla pro uživatelské účty

5.1 Pro přístup k některým prostředkům správce zřizuje uživateli uživatelský účet. Uživatelský účet je vždy identifikován jménem a příjmením uživatele a smí jej používat pouze osoba, pro kterou byl zřízen.

5.2 Uživatelský účet může být zřízen pouze na dobu nezbytnou pro provádění činností sjednaných ve zvláštní smlouvě.

5.3 Zřízení a změny uživatelských účtů schvaluje vždy bezpečnostní správce. Ten ověřuje, že byly splněny podmínky udělení přístupu uživateli, zejména, že jsou se zpracovatelem řádně uzavřeny smlouvy o ochraně informací.

5.4 Žádost o zřízení nebo změnu uživatelského účtu podává uživatel. Vzor žádosti stanoví bezpečnostní správce.

5.5 V případě zřízení nového uživatelského účtu předá správce uživateli jeho identifikační údaje: přihlašovací jméno a jednorázové heslo, které si musí uživatel po prvním přihlášení změnit.

5.6

5.7 Identifikační údaje k uživatelskému účtu, zejména přístupové heslo, musí uživatel udržovat v tajnosti a nesmí je poskytovat žádným dalším osobám.

5.8 Identifikační údaje k uživatelskému účtu, zejména přístupové heslo, uživatel nesmí zapisovat na lehce přístupná místa. V případě, že si chce pro vlastní potřebu uložit záznam o přihlašovacích údajích, musí to učinit tak, aby nebyl přístupný žádné jiné osobě.

5.9 Uživatel nesmí umožnit žádné další osobě pracovat s prostředky správce prostřednictvím svého uživatelského účtu.

5.10 V případě podezření na vyzrazení hesla je uživatel povinen neprodleně své heslo změnit.

5.11 Požadavky na kvalitu přístupového hesla:

a) Minimální délka: 8 znaků;

b) Minimální složitost (komplexita): alespoň jeden znak z každé skupiny: velká písmena, malá písmena, číslice.

5.12 Uživatelský účet smí být aktivní pouze na dobu nezbytnou pro provedení sjednaného úkonu. Mimo tuto dobu bude účet znepřístupněn.

5.13 Uživatel je povinen vždy předem informovat správce o termínu zahájení provádění sjednaného výkonu. Na základě toho mu správce zpřístupní jeho uživatelský účet.

5.14 Uživatel je povinen vždy bezodkladně informovat správce o skončení provádění sjednaného výkonu. Na základě toho mu správce znepřístupní jeho uživatelský účet.

Článek 6
Pokyny správce

6.1 Uživatel je povinen dbát všech pokynů správce v souvislosti s provozem prostředků. Pokyny zasílané e-mailem musí být důvěryhodné, tzn., že jsou opatřeny kvalifikovaným elektronickým podpisem.

6.2 Pokyny, které nejsou zajištěny způsobem dle předchozího odstavce, musí být uživatelem považovány za nedůvěryhodné a uživatel je povinen jejich pravost ověřit.

6.3 Pokyny správce nesmí být v rozporu s touto bezpečnostní směrnicí, zvláštní smlouvou, smlouvou o ochraně informací nebo jinými právními předpisy. V případě, že pokyny nesplňují tento

požadavek, uživatel se těmito pokyny neřídí a o přijetí takových pokynů informuje bezpečnostního správce.

Článek 7
Podmínky přístupu k prostředkům správce

7.1 Uživatelé jsou povinni:

a) využívat přidělený přístup k prostředkům správce pouze pro plnění předmětu zvláštní smlouvy, a to v souladu se smluvním ujednáním;

b) konzultovat se správcem veškeré změny v prostředcích a jejich nastavení, které jsou nutné pro provedení sjednaného úkonu a implementovat je až po jejich vzájemném odsouhlasení;

c) provádění sjednaného úkonu může probíhat jen s vědomím správce, který je v případě potřeby fyzického přístupu k informacím a prostředkům vybaví identifikační kartou „SERVIS“. Tuto kartu musí nosit uživatel viditelně po celou dobu provádění sjednaného úkonu;

d) po skončení sjednaného úkonu informovat správce o skutečně provedených úkonech a předat mu aktualizovanou provozní dokumentaci, pokud došlo v důsledku provedených úkonů k její změně.

7.2 Uživatelům je zakázáno:

a) bez vědomí správce jakkoliv přistupovat k informacím nebo prostředkům správce;

b) jakkoliv neoprávněně manipulovat s informacemi nebo prostředky správce.; neoprávněnou manipulací se rozumí vše, co bezprostředně nesouvisí s plněním předmětu zvláštní smlouvy;

c) obcházet zabezpečení informací a prostředků a zneužívat zjištěných slabin v jejich zabezpečení;

d) používat jiné prostředky vlastní nebo cizí, pokud tyto prostředky neslouží k plnění předmětu zvláštní smlouvy;

e) provádět jiné aktivity, než ty, které jsou vymezeny zvláštní smlouvou.

7.3 Uživatelé si musí být vědomi toho, že jejich činnost v rámci prostředků správce může být monitorována a logována.

7.4 Veškeré sjednané úkony, které vyžadují přítomnost uživatele v chráněných zónách správce (serverovna apod.), smějí být prováděny pouze za přítomnosti správcem určené osoby.

Článek 8
Podmínky vzdáleného přístupu

8.1 Uživatel, který přistupuje k prostředkům správce vzdáleně, musí zajistit bezpečnost a ochranu prostředí, z něhož vzdáleně přistupuje. Zejména je povinen zajistit, že

a) prostředky, z nichž vzdáleně přistupuje, nejsou napadeny škodlivým kódem a je na nich nainstalována funkční a aktuální antivirová ochrana,

b) prostředky, z nichž vzdáleně přistupuje, jsou plně pod jejich kontrolou, tzn., že k těmto prostředkům nemá přístup žádná jiná osoba,

c) v prostředcích, ze kterých uživatel vzdáleně přistupuje, ani na jiná úložiště nebudou bez souhlasu správce ukládány žádné informace získané z prostředků správce,

d) celá komunikace vzdáleného přístupu probíhá šifrovaně prostřednictvím zabezpečeného protokolu (např. https).

8.2 Uživatel nesmí používat pro vzdálený přístup veřejné prostředky a prostředky zapůjčené od jiných neznámých osob.

Článek 9
Hlášení poruch a závad

9.1 Uživatel je povinen hlásit poruchy a závady na prostředcích správce správci. Poruchy se oznamují e-mailem nebo telefonicky.

9.2 Uživatel je povinen účinně spolupracovat se správcem při odstraňování poruch a závad a dodržovat jeho pokyny.

Článek 10
Bezpečnostní události, incidenty a slabiny

10.1 Uživatel je povinen neprodleně oznámit správci všechny zjištěné bezpečnostní události, incidenty a slabiny nebo podezření na ně.

10.2 Hlášení bezpečnostních událostí, incidentů a slabin je možné písemně e-mailem, telefonicky nebo osobně. Příjemce oznámení je povinen oznamovateli písemně e-mailem potvrdit přijetí jeho oznámení. Ohlašovací povinnost uživatele je splněna, pokud bylo hlášení bezpečnostní události, incidentu nebo slabiny písemně e-mailem potvrzeno příjemcem oznámení.

10.3 Uživatel nesmí o bezpečnostních událostech, incidentech a slabinách informovat žádnou jinou osobu.

10.4 Uživatel je povinen účinně spolupracovat se správcem při řešení bezpečnostních událostí, incidentů a slabin, zejména poskytovat jim úplné a pravdivé informace a dodržovat jeho pokyny.

Článek 11
Porušení povinností vyplývajících z bezpečnostní směrnice

11.1 Porušení povinností vyplývajících z této bezpečnostní směrnice bude posuzováno jako zvláště závažné porušení zvláštní smlouvy a smlouvy o ochraně informací.

11.2 Na základě individuálního posouzení závažnosti, míry zavinění a konkrétního rizika, případně míry dopadu a následků bezpečnostního incidentu způsobeného porušením výše uvedených bezpečnostních předpisů uživatelem, budou uskutečněna potřebná opatření v souladu s uzavřenou smlouvou. Tím není dotčena případná trestně právní odpovědnost uživatele či zpracovatele.

Článek 12
Verze a schvalovací doložka

12.1 Tato Bezpečnostní směrnice pro dodavatele (verze 4) ruší Bezpečnostní směrnici pro dodavatele (verze 3), kterou vydala Rada města Karviné dne 21. 06. 2017.

12.2 Tato Bezpečnostní směrnice pro dodavatele (verze 4) byla schválena Radou města Karviné dne 28. 05. 2018, č. usnesení 4757 s účinností od 29. 05. 2018.

Ing. Jan Wolf v. r.
primátor

Karel Wiewiórka v. r.
náměstek primátora