Zveřejnění poskytnutých informací dle § 5 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Žádost č. 46/2020 ze dne 4.11.2020

informace k disciplinárním řízením

Vyřizoval: Odbor organizační

TEXT ODPOVĚDI

K Vaší žádosti sdělujeme následující:

1) Zaslání veškerých vnitřních předpisů, které se vztahují k ustanovování a činnosti disciplinární komise (disciplinárních komisí) – Bezpečnostní politika informací SMK - Celková bezpečnostní politika informací (verze 4) (viz Příloha k tomuto Sdělení)

2) statistické údaje o činnosti disciplinárních komisí v posledních třech letech (tj. od 28.10.2017 do 28.10.2020), a to konkrétně kolikrát byly svolány – od roku 2017 bylo na Magistrátu města Karviná svoláno 5 x disciplinární řízení

3) kolik jednotlivých případů (spisů) týkajících se zaměstnanců vedly během jednotlivých čtvrtletí, a to s rozdělením na úřednické a neúřednické zaměstnance a s jakým výsledkem

- 2. čtvrtletí 2017 – 2x, oba úředníci, oba písemné upozornění na porušení právních předpisů
- 3. čtvrtletí 2017 – 1x, úředník, písemné upozornění na porušení právních předpisů
- 1. čtvrtletí 2020 – 1x, neúředník, písemné upozornění na porušení právních předpisů
- 3. čtvrtletí 2020 – 1x, úředník, pracovněprávní úkon

4) údaje o členech disciplinární komise v průběhu času (postačí anonymizovaně, tj. uvedení např. „člen A od 1.1.2017 do 31.12.2019“ apod.).

- člen A 01. 01. 2017 – dosud
- člen B 01. 01. 2017 – dosud
- člen C 29. 05. 2018 – dosud

- ostatní členové dle článku 22.3.1 Bezpečnostní politiky informací SMK - Celková bezpečnostní politiky informací (verze 4)

Bezpečnostní politika informací SMK

Celková bezpečnostní politika informací (verze 4)

ČÁST I.

ÚVODNÍ USTANOVENÍ

Článek 1

Termíny a definice

1.1 Aktivum = vše, co má pro organizaci, její působnost a funkci nějakou hodnotu a je předmětem ochrany podle této bezpečnostní politiky;

1.2 Autentizace = proces ověření proklamované identity subjektu (uživatele);

1.3 Autorizace = proces ověření oprávnění a umožnění přístupu či provedení konkrétní operace daným subjektem (uživatelem);

1.4 Data = záznamy nebo údaje v digitálním tvaru, jež jsou nositeli informace;

1.5 Datová síť = soubor vzájemně propojených ICT zařízení v organizaci, které realizují spojení a výměnu informací mezi nimi;

1.6 Informace = vědění, které lze předávat jako obsah zprávy či sdělení;

1.7 ICT = informační a komunikační technologie;

1.8 ICT prostředky (také "prostředky pro zpracování informací") = veškeré programové a technické vybavení, které je provozováno za účelem zpracování a ukládání informací;

1.9 Informační systém (také "IS") = programové vybavení, které slouží ke sběru, zpracování a ukládání informací;

1.10 Hardware = technické vybavení, zahrnující počítače, tiskárny, skenery, monitory atd.

1.11 Organizace = orgán města nebo příspěvková organizace, v níž se uplatňuje tato bezpečnostní politika.

1.12 Software = programové vybavení, zahrnující aplikace, informační systémy, operační systémy atd.

1.13 Škodlivý kód (také "malware") = počítačový program určený ke vniknutí do počítačového systému, získání neoprávněného přístupu k informacím nebo poškození počítačového systému; patří sem zejména počítačové viry, červi, trojské koně, spyware, adware, ransomware atd.

1.14 Uživatel = osoba s oprávněním přistupovat k určeným aktivům organizace;

1.15 Zaměstnanec = osoba v zaměstnaneckém nebo jiném poměru k organizaci;

Článek 2

Preambule

2.1 Rada města Karviné vydává tuto Bezpečnostní politiku informací statutárního města Karviné (dále jen "bezpečnostní politika"), kterou deklaruje svůj záměr podporovat cíle a principy informační a kybernetické bezpečnosti.

2.2 Cílem této bezpečnostní politiky je zavést závazné principy informační a kybernetické bezpečnosti, minimalizovat bezpečnostní rizika a stanovit technické a organizační opatření k zajištění ochrany osobních údajů v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (dále jen "GDPR"). Cílem této bezpečnostní politiky je také aplikovat vhodná opatření dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen "ZoKB"), která lze oprávněně požadovat k zajištění kybernetické bezpečnosti v organizaci.

2.3 Tato bezpečnostní politika se uplatňuje ve všech orgánech města (tj. Magistrát města Karviné a Městská policie Karviná) a příspěvkových organizacích zřízených statutárním městem Karviná.

Článek 3

Definice informační a kybernetické bezpečnosti

3.1 Informace dle této bezpečnostní politiky přestavuje jakékoliv vědění, které lze předávat jako obsah zprávy či sdělení. Obsahem informace mohou být též osobní údaje dle GDPR.

3.2 Informační bezpečnost představuje ochranu informací ve všech jejich formách a po celý jejich životní cyklus, tedy během jejich vzniku, zpracování, ukládání, přenosu a likvidace.

3.3 Předmětem ochrany z pohledu informační bezpečnosti jsou informace bez ohledu na způsob jejich výskytu. Vztahuje se tedy na všechny informace v digitální či analogové podobě, ve formě písemné, hlasové nebo jiné (např. ve formě myšlenky).

3.4 Dosažení informační bezpečnosti je zajištěno třemi základními principy, tzv. atributy informační bezpečnosti:

a) Důvěrnost = ochrana před neoprávněným přístupem,

b) Dostupnost = zajištění odpovídajícího přístupu k informacím oprávněným osobám tak, že jsou jim dostupné, kdykoliv je potřebují,

c) Integrita = ochrana před neoprávněnými úpravami nebo zničením.

3.5 Kybernetická bezpečnost je zaměřena na ochranu informací zpracovávaných pomocí prostředků ICT. Je tedy podmnožinou informační bezpečnosti.

Článek 4

Cíle a oblasti bezpečnostní politiky

4.1 Hlavním cílem informační a kybernetické bezpečnosti dle této bezpečnostní politiky je zajištění trvalé a kvalitní podpory činností organizace s využitím ICT a ochrana důvěrnosti, dostupnosti a integrity informací v organizaci.

4.2 Dalším cílem informační a kybernetické bezpečnosti dle této bezpečnostní politiky je ochrana všech prostředků pro zpracování informací a dalších aktiv organizace, které mohou mít vliv na bezpečnost informací v organizaci.

4.3 Základní oblasti informační a kybernetické bezpečnosti, kterými se tato bezpečnostní politika zabývá, jsou:

a) Politika bezpečnosti ICT

b) Organizace bezpečnosti

c) Klasifikace a řízení aktiv

d) Bezpečnost lidských zdrojů

e) Fyzická bezpečnost a bezpečnost prostředí

f) Řízení komunikací a řízení provozu

g) Řízení přístupu

h) Nákup, vývoj a údržba informačního systému

i) Zvládání bezpečnostních incidentů

j) Soulad s požadavky

ČÁST II.

BEZPEČNOSTNÍ POLITIKA

Článek 5

Dokumenty bezpečnostní politiky

5.1 Bezpečnostní politika je tvořena soustavou závazných dokumentů (zásad), které vymezují pravidla, metody, povinnosti a odpovědnosti pro přístup a nakládání s informacemi a prostředky pro zpracování informací v organizaci.

5.2 Identifikace dokumentů:

a) Celková bezpečnostní politika informací

b) Bezpečnostní směrnice pro správce ICT

c) Bezpečnostní směrnice pro externí uživatele

d) Bezpečnostní směrnice pro dodavatele

e) Provozní a bezpečnostní směrnice Technologického centra Karviná

5.3 Celková bezpečnostní politika informací stanovuje základní rámec informační a kybernetické bezpečnosti, definuje základní pojmy a procesy řízení bezpečnosti informací a stanovuje konkrétní povinnosti a odpovědnosti interních uživatelů. Je závazná pro všechny zaměstnance a osoby, kterým byl umožněn přístup k informacím a aktivům organizace na základě zaměstnaneckého nebo obdobného poměru s organizací a dále pro uvolněné členy Zastupitelstva města Karviné (dále jen "vedení města").

5.4 Bezpečnostní směrnice pro správce ICT stanovuje detailní procesy řízení bezpečnosti a konkrétní povinnosti a odpovědnosti osob, které se podílejí na zajištění správy a provozu ICT v organizaci. Je závazná pro všechny osoby, které vykonávají činnost bezpečnostního správce, systémového inženýra, správce ICT a lokálního správce.

5.5 Bezpečnostní směrnice pro externí uživatele stanovuje konkrétní povinnosti a odpovědnosti externích uživatelů. Je závazná pro neuvolněné členy Zastupitelstva města Karviné, případně jiné osoby, kterým byl umožněn přístup k informacím a aktivům organizace.

5.6 Bezpečnostní směrnice pro dodavatele stanovuje konkrétní povinnosti a odpovědnosti dodavatelů a jejich zaměstnanců. Je závazná pro všechny osoby, kterým byl umožněn přístup k informacím a aktivům organizace na základě servisní, dodavatelské nebo jiné smlouvy.

5.7 Provozní a bezpečnostní směrnice Technologického centra Karviná stanovuje podmínky provozu a povinnosti uživatelů Technologického centra Karviná (dále jen "TCK"). Je závazná pro všechny uživatele TCK, kterým byl umožněn přístup k aplikacím poskytovaným prostřednictvím TCK.

Článek 6

Řízení změn v dokumentech a označování dokumentů

6.1 Změny v dokumentech bezpečnostní politiky budou probíhat vydáváním nových verzí, které se budou označovat pořadovým číslem. Číslo verze je společné pro všechny dokumenty bezpečnostní politiky (tzv. verze bezpečnostní politiky). Všechny dokumenty bezpečnostní politiky musí být proto schvalovány společně.

6.2 Každý dokument bezpečnostní politiky bude označen číslem verze bezpečnostní politiky, které bude součástí názvu dokumentu.

Článek 7

Schvalovací procesy

7.1 Všechny dokumenty bezpečnostní politiky

a) zpracovává bezpečnostní správce,

b) schvaluje Rada města Karviné.

Článek 8

Platnost a závaznost

8.1 Bezpečnostní politika (tzn. všechny její dokumenty) je platná schválením Radou města Karviné a účinnosti nabývá následující pracovní den po jejím schválení.

8.2 Tato bezpečnostní politika je závazná pro všechny, kterým byl udělen přístup k informacím a prostředkům pro zpracování informací v organizaci.

8.3 Všechny osoby s přístupem k informacím a ICT prostředkům organizace musí být prokazatelně seznámeny s aktuální verzí bezpečnostní politiky v rozsahu závaznosti jednotlivých dokumentů dle odst. 5.3 až 5.7. Za to odpovídá ředitel organizace nebo tajemník MMK.

Článek 9

Přezkoumání bezpečnostní politiky

9.1 Pro zajištění aktuálnosti bezpečnostní politiky bude probíhat její revize vždy 1x ročně, zpravidla v prosinci. Aktualizace bezpečnostní politiky bude probíhat vydáváním nových verzí. Vydání nové verze bezpečnostní politiky není vázáno na její pravidelnou revizi. Nová verze bezpečnostní politiky může být vydána kdykoliv, dojde-li k zásadním změnám ovlivňujícím platnou bezpečnostní politiku. Za provádění pravidelné revize a aktualizaci bezpečnostní politiky je odpovědný bezpečnostní správce.

ČÁST III.

ORGANIZACE BEZPEČNOSTI

Článek 10

Interní organizace

10.1 Odpovědnou osobou za informační a kybernetickou bezpečnost v organizaci je ředitel organizace nebo tajemník MMK. Jejich pravomoc je především rozhodovací. Při uplatňování systému řízení informační a kybernetické bezpečnosti úzce spolupracují s bezpečnostním správcem.

10.2 Pro zajištění informační a kybernetické bezpečnosti jsou stanoveny následující role a odpovědnosti.

10.3 Bezpečnostní správce

10.3.1 Bezpečnostní správce je garantem dokumentů bezpečnostní politiky a je odpovědný za implementaci systému řízení informační a kybernetické bezpečnosti v organizaci. Při své činnosti koordinuje činnost správců ICT. Za svou činnost odpovídá Radě města Karviné. Jeho povinností je minimálně 1x ročně provádět kontrolu souladu bezpečnostní politiky s právními předpisy a navrhovat její aktualizaci.

10.3.2 Bezpečnostním správcem je vedoucí oddělení informačních služeb Odboru organizačního. Bezpečnostní správce může pověřit výkonem některých činností dle této bezpečnostní politiky také jiného zaměstnance organizace v souladu s touto bezpečnostní politikou.

10.3.3 Role bezpečnostního správce dle této bezpečnostní politiky odpovídá roli manažera kybernetické bezpečnosti dle ZoKB.

10.4 Systémový inženýr

10.4.1 Systémový inženýr je určený zaměstnanec oddělení informačních služeb MMK a je odpovědný za návrh a implementaci bezpečnostních opatření (od infrastruktury až po bezpečnost na aplikační úrovni). Prosazuje bezpečnost informací v rámci koncepčního rozvoje informačních a komunikačních systémů.

10.4.2 Role systémového inženýra odpovídá roli architekta kybernetické bezpečnosti dle ZoKB.

10.5 Správce ICT

10.5.1 Správce ICT je určený zaměstnanec oddělení informačních služeb MMK, který je odpovědný za správu a provoz jemu svěřených ICT prostředků v souladu s bezpečnostní politikou.

10.5.2 Správce ICT odpovědný za správu a provoz informačních systémů, provozovaných v datové síti organizace je označován také jako "správce aplikací". Odpovídá za správné nastavení bezpečnostních mechanismů a přístupových práv v informačních systémech dle bezpečnostní politiky. U informačních systémů, které jsou informačními systémy veřejné správy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, vykonává správce aplikací také činnosti správce informačních systémů veřejné správy dle tohoto zákona.
Určení správců aplikací pro jednotlivé informační systémy je součástí evidence informačních aktiv.

10.5.3 Správce ICT odpovědný za správu a provoz celé infrastruktury svěřené datové sítě organizace a jejich koncových stanic je označován také jako "správce datové sítě". Odpovídá za správné nastavení bezpečnostních mechanismů a přístupových práv v datové síti dle bezpečnostní politiky.

10.5.4 Správce ICT odpovědný za správu a provoz databází provozovaných v datové síti organizace je označován také jako "správce databáze". Odpovídá za správné nastavení bezpečnostních mechanismů a přístupových práv dle bezpečnostní politiky.

10.5.5 Správce ICT odpovědný za správu a provoz bezpečnostních systémů MPK (Městský kamerový dohlížecí systém a Pult centralizované ochrany) je označován také jako "správce bezpečnostních systémů MPK". Odpovídá za správné nastavení bezpečnostních mechanismů a přístupových práv k těmto systémům dle bezpečnostní politiky.

10.5.6 Činnosti jednotlivých správců mohou být kumulovány. V takovém případě se dále používá souhrnného označení "správce ICT".

10.5.7 Správce ICT odpovídá za svou činnost systémovému inženýrovi.

10.6 Lokální administrátor

10.6.1 Lokální administrátor je určený zaměstnanec organizace, kterého pověřil správce ICT výkonem některých činností při zajištění správy a provozu ICT.

10.6.2 Pro lokálního administrátora platí odpovědnosti správce ICT přiměřeně v rozsahu jemu svěřených činností.

10.6.3 Lokální administrátor za svou činnost odpovídá správci ICT.

10.7 Správce majetku

10.7.1 Správce majetku je určený zaměstnanec organizace a odpovídá za správnou evidenci přiřazených ICT prostředků zaměstnancům organizace.

10.7.2 V příspěvkové organizaci správce majetku odpovídá také za provedení inventarizace zapůjčených ICT zařízení, která jsou v majetkové evidenci MMK.

10.8 Garant aktiv

10.8.1 Garant aktiv je určený zaměstnanec organizace a je odpovědný za klasifikaci informací, ohodnocení aktiva a stanovení požadavků na přiměřenou ochranu aktiva. Garant softwarových a informačních aktiv je také odpovědný za určení účelu a způsobu zpracování a ukládání informací a stanovení podmínek přístupu k nim.

10.9 Uživatel

10.9.1 Uživatelem je každá osoba, jíž byl umožněn přístup k informacím, ICT prostředkům nebo do datové sítě organizace. Uživateli mohou být:

a) zaměstnanci statutárního města Karviné, zařazení do MMK (interní uživatelé),

b) zaměstnanci statutárního města Karviné, zařazení do MPK (interní uživatelé),

c) zaměstnanci příspěvkových organizací zřízených Statutárním městem Karviná (interní uživatelé)

d) zaměstnanci na dohodu nebo jiní externí zaměstnanci (interní uživatelé),

e) osoby vykonávající v organizaci rekvalifikaci v rámci uzavřené dohody o zabezpečení odborné praxe (interní uživatelé),

f) primátor a náměstci (interní uživatelé),

g) zastupitelé a radní (externí uživatelé),

h) zaměstnanci obcí ve správním obvodu ORP Karviná (uživatelé TCK),

i) zaměstnanci servisních a dodavatelských firem nebo jiné osoby (dodavatelé).

10.9.2 Všichni uživatelé bez ohledu na pracovní zařazení, zastávané funkce či role jsou odpovědní za dodržování bezpečnostní politiky a nesou odpovědnost za škody vzniklé nedodržením nebo porušením pravidel vyplývajících z bezpečnostní politiky.

10.10 Klient

10.10.1 Klientem je fyzická osoba, která využívá služeb organizace a přitom nespadá do role uživatele dle předchozího odstavce. Jedná se zejména o občany (klienty MMK a MPK), žáky (klienty ZŠ/MŠ), čtenáře (klienty RKK), návštěvníky kulturních akcí (klienty MDK), příjemce sociálních služeb (klienty SSK) atd.

10.10.2 Klient může získat omezený přístup k informacím, ICT prostředkům nebo do datové sítě organizace za podmínek vymezených touto bezpečnostní politikou.

10.11 Pověřenec

10.11.1 Pověřenec je určený zaměstnanec, zařazený do Odboru organizačního, oddělení právního a kontrolního MMK, který plní úkoly pověřence na ochranu osobních údajů dle čl. 39 GDPR.

10.11.2 Pověřenec je společný pro všechny organizace, ve kterých se uplatňuje tato bezpečnostní politika.

Článek 11

Dohody o ochraně informací

11.1 Povinnosti uživatelů dle odst. 10.9.1 písm a) až d) v souvislosti s ochranou informací vyplývají ze zvláštních právních předpisů a vnitřních předpisů.

11.2 S uživateli dle odst. 10.9.1 písm. e) a g) se uzavírají smlouvy o ochraně informací a přístupu do datové sítě. Obsah a formu dohody stanovuje bezpečnostní správce.

11.3 Za uzavírání smluv s uživateli dle odst. 10.9.1 písm. e) odpovídá oddělení informačních služeb Odboru organizačního.

11.4 Za uzavírání smluv s uživateli dle odst. 10.9.1 písm. f) a g) odpovídá oddělení Kancelář primátora.

11.5 Smlouvy o ochraně informací a přístupu do datové sítě uzavírá ředitel organizace nebo Odbor organizační MMK. Tyto smlouvy jsou ukládány u bezpečnostního správce.

Článek 12

Kontakt s orgány veřejné správy

12.1 Bezpečnostní správce a pověřenec se v rámci své činnosti účastní potřebných jednání s orgány veřejné správy.

12.2 Pověřenec spolupracuje s dozorovým orgánem při ochraně osobních údajů dle GDPR.

12.3 Bezpečnostní správce je členem krizového štábu statutárního města Karviné.

12.4 O podání trestního oznámení v případě podezření na porušení právních předpisů v oblasti informační a kybernetické bezpečnosti rozhoduje Rada města Karviné na návrh bezpečnostního správce nebo pověřence.

Článek 13

Kontakt se zájmovými skupinami

13.1 Bezpečnostní správce, systémový inženýr, správci ICT a lokální administrátoři si musí průběžně rozšiřovat znalosti o nejlepších praktikách a nejnovějších trendech v oblasti bezpečnosti informací a kybernetické bezpečnosti tak, aby je byli schopni aplikovat do jimi spravovaných oblastí a systémů. Za tím účelem jim organizace umožní účastnit se různých odborných fór, konferencí a školení.

13.2 V případě přetrvávajícího bezpečnostního incidentu může bezpečnostní správce určit, že se na jeho řešení budou podílet i jiné zájmové skupiny, zejména národní CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team).

Článek 14

Nezávislá přezkoumání bezpečnosti informací

14.1 Iniciovat nezávislé přezkoumání bezpečnosti informací může kdykoliv vedení města, ředitel organizace, tajemník MMK, pověřenec nebo bezpečnostní správce. O záměru zahájit přezkum musí ten, kdo přezkum iniciuje, předem informovat bezpečnostního správce.

14.2 Výsledky přezkumu bezpečnosti informací musí být předány bezpečnostnímu správci neprodleně po jeho dokončení. Bezpečnostní správce je povinen informovat Radu města Karviné o výsledcích provedeného přezkumu a navrhnout opatření ke zjištěním přezkumu.

14.3 Nezávislé přezkoumání by mělo proběhnout alespoň jednou za čtyři roky.

Článek 15

Externí subjekty

15.1 Bezpečnostní požadavky pro přístup dodavatelů

15.1.1 Dodavatelé mohou získat přístup ICT prostředkům a informacím prostřednictvím datové sítě organizace na základě řádně uzavřené dodavatelské smlouvy a uzavřené smlouvy o ochraně informací a přístupu do datové sítě.

15.1.2 Dodavatelskou smlouvu uzavírá organizace s dodavatelem zpravidla v režimu kupní smlouvy nebo smlouvy o dílo. Za dodavatelskou smlouvu se považuje také jednorázová objednávka na dodávky a služby vystavená organizací.

15.1.3 Smlouvu o ochraně informací a přístupu do datové sítě s dodavateli uzavírá Odbor organizační MMK a může se uzavírat buď jednotlivě s fyzickými osobami, nebo s právnickou osobou. Tyto smlouvy jsou ukládány u bezpečnostního správce a jejich stejnopis nebo kopie také u organizace, pokud je dodavatelský vztah uzavřen s organizací.

15.1.4 Postupy pro schvalování přístupů, zřizování uživatelských účtů a povinnosti dodavatelů jsou uvedeny v Bezpečnostní směrnici pro dodavatele.

15.1.5 Za plnění bezpečnostních opatření dle odst. 15.1.1 až 15.1.3 odpovídá ředitel organizace nebo vedoucí odboru MMK, kde se uzavírá dodavatelská smlouva a bezpečnostní správce.

15.2 Bezpečnostní požadavky pro přístup externích uživatelů

15.2.1 Neuvolněným členům Zastupitelstva města Karviné (dále jen "zastupitelé") může být umožněn přístup k ICT prostředkům pouze po dobu jejich mandátu. Rozsah přístupu jim musí být omezen pouze na prostředky a informace nezbytné pro výkon funkce zastupitele dle zákona č. 128/2000 Sb., o obcích.

15.2.2 Se zastupiteli se uzavírají dohody o ochraně informací a přístupu do datové sítě. Obsah a formu dohody stanovuje bezpečnostní správce.

15.2.3 Jiným osobám může být udělen přístup k informacím a ICT prostředkům pouze na základě zvláštní smlouvy schválené Radou města Karviné. V takové smlouvě pak musí být přesně vymezen rozsah a účel přístupu k ICT prostředkům a stanovena povinnost dodržovat Bezpečnostní směrnici pro externí uživatele, případně další povinnosti stanovené bezpečnostním správcem. Bezpečnostní správce je připomínkovým místem těchto smluv. Kopie nebo stejnopis smlouvy se ukládají též u bezpečnostního správce.

15.2.4 Za plnění bezpečnostních opatření dle odst. 15.2.1 až 15.2.3 odpovídá oddělení Kancelář primátora MMK.

15.3 Bezpečnostní požadavky pro přístup uživatelů Technologického centra Karviná

15.3.1 Technologické centrum Karviná poskytuje informační služby formou hostingu vybraných informačních systémů z datové sítě MMK. Rozsah, způsob poskytování těchto služeb a povinnosti jejich uživatelů jsou definovány v Provozní směrnici

Technologického centra Karviná.

15.3.2 Informační systémy poskytované TCK musí být provozovány samostatně a vždy odděleně od jiných informačních systémů provozovaných v datové síti MMK. Klientům TCK nesmí být umožněn přímý přístup do datové sítě MMK, uživatelské účty jsou jim zřizovány pouze v jednotlivých informačních systémech, do kterých přistupují prostřednictvím publikovaného rozhraní příslušného informačního systému.

15.3.3 Uživatelům TCK není umožněn přístup k informacím žádné organizace a proto se s nimi dohoda o ochraně informací neuzavírá.

15.3.4 Za plnění bezpečnostních opatření dle odst. 15.3.1 a 15.3.2 odpovídá systémový inženýr.

15.4 Bezpečnostní požadavky pro přístup klientů

15.4.1 Klienti smí mít přístup k informacím pouze v zákonem stanoveném rozsahu (zejména dle GDPR, Správního řádu, Zákona o svobodném přístupu k informacím, atd.). Za tímto účelem smí získat přístup k informacím a ICT prostředkům v omezeném rozsahu.

15.4.2 Klientům nesmí být umožněn přístup k informacím týkajícím se jiného určeného nebo určitelného subjektu dle GDPR, pokud jiný právní předpis nestanoví jinak.

15.4.3 Za plnění bezpečnostních opatření dle odst. 15.4.1 a 15.4.2 odpovídají všichni uživatelé uvedení odst. 10.9.1 písm. a) až f).

15.4.4 Za stanovení požadavků na ochranu hardwarových prostředků určených pro použití klienty a jejich implementaci odpovídá systémový inženýr.

15.4.5 Za stanovení požadavků na ochranu softwarových prostředků určených k použití klienty a informací odpovídají garanti příslušných aktiv a za jejich implementaci odpovídá správce ICT.

Článek 16

Odpovědnosti uživatelů

16.1 Uživatelé musí aktivně spolupracovat při naplňování cílů informační bezpečnosti, zejména dodržováním bezpečnostní politiky. Každý uživatel je osobně odpovědný za dodržování bezpečnostní politiky.

16.2 Uživatelé odpovídají za to, že zpracovávají osobní údaje v souladu s GDPR.

ČÁST IV.

ŘÍZENÍ AKTIV

Článek 17

Skupiny aktiv

17.1 V organizaci jsou definovány následující skupiny aktiv:

	Fyzická aktiva	Softwarová aktiva	Informační aktiva
Primární aktiva	---	informační systémy	data informačních systémů, jiné informace a informační zdroje
Podpůrná aktiva	hardware počítačů a příslušenství, servery, datové sítě vč. kabeláže, aktivních a pasivních prvků	virtuální servery a stanice, operační systémy, desktopové aplikace, správcovské systémy	---

Článek 18

Odpovědnost za aktiva

18.1 Evidence aktiv

18.1.1 Všechna fyzická, softwarová a informační aktiva musí být identifikována a evidována.

18.1.2 Odpovědnost za evidenci softwarových aktiv má správce ICT.

18.1.3 Odpovědnost za evidenci informačních aktiv má garant aktiva.

18.1.4 Odpovědnost za evidenci fyzických aktiv má správce majetku.

18.2 Vlastnictví aktiv

18.2.1 Každé z aktiv musí mít přiřazeného garanta. Odpovědnosti garanta jsou definovány v odst. 10.8 a násl.

18.2.2 Garanta informačních aktiv určuje ředitel organizace nebo tajemník MMK a zpravidla je jím vedoucí zaměstnanec, na jehož organizační jednotce aktivum vzniklo.

18.2.3 Garanta softwarových aktiv určuje bezpečnostní správce.

18.2.4 Garantem fyzických (HW) aktiv je systémový inženýr.

18.3 Přípustné použití aktiv
Pravidla pro přípustné použití informací a aktiv jsou definována dále v této Celkové bezpečnostní politice informací (ČÁST VIII. až ČÁST X.), v Bezpečnostní směrnici pro externí uživatele a Bezpečnostní směrnici pro dodavatele. Tato pravidla jsou závazná pro příslušnou skupinu uživatelů.

Článek 19

Schvalovací proces prostředků pro zpracování informací

19.1 Každý nový prostředek pro zpracování informací, ať už jde o hardware nebo software musí být předem schválen pro použití v datové síti organizace. Schvalování probíhá změnovým řízením, které je definováno v článku 9 Bezpečnostní směrnice pro správce ICT.

19.2 Použití soukromých ICT prostředků (počítače, notebooky, tablety, chytré telefony apod.)

19.2.1 Použití soukromých ICT prostředků v datové síti MMK interními uživateli je možné pouze v bezdrátové síti (WiFi) v rámci systému BYOD (Bring Your Own Device, tj. "přines si své vlastní zařízení"). Uživatel si zaregistruje své zařízení v systému BYOD.

19.2.2 Použití soukromých ICT prostředků v ostatních datových sítích organizací je možné po předchozím schválení. Žádost se podává prostřednictvím systému Helpdesk. Použití soukromých ICT prostředků schvaluje správce ICT.

19.2.3 Použití soukromých ICT prostředků v datové síti organizace interními uživateli je možné pouze v souladu s Celkovou bezpečnostní politikou informací.

19.2.4 Použití soukromých ICT prostředků v datové síti organizace dodavateli je možné v souladu s Bezpečnostní směrnicí pro dodavatele.

19.2.5 Použití soukromých ICT prostředků v datové síti organizace externími uživateli je možné v souladu s Bezpečnostní směrnicí pro externí uživatele.

Článek 20

Klasifikace informací

20.1 Každá informace musí být zařazena do jedné ze čtyř tříd klasifikace informací. Třídy klasifikace určují důvěrnost informací a stupeň požadovaného zabezpečení. Každý uživatel musí znát stupeň klasifikace informací, se kterými přichází do styku. Za zařazení informace do stupně klasifikace odpovídá garant příslušného informačního aktiva.

20.2 V organizacích byly stanoveny následující třídy klasifikace informací ve vazbě na Národní standard elektronických systémů spisové služby (NSESSS):

Stupeň	Označení	Popis	Vazba na NSESSS1)
1	Veřejné	Veřejně přístupné informace, např. informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím nebo dle Správního řádu (zákon č. 500/2004 Sb.), v platném znění. Tyto informace nevyžadují zvláštní úroveň ochrany z pohledu důvěrnosti. (Je však nutné dbát na jejich ochranu z pohledu integrity, aby nedošlo ke zveřejnění informací, které neodpovídají skutečnosti.)	Veřejný

2	Interní	Informace přístupné všem zaměstnancům organizace pro výkon jejich pracovních a jiných povinností. Veškeré informace, které nesplňují kritéria pro klasifikaci CHRÁNĚNÉ nebo NEVEŘEJNÉ a současně nejsou určeny ke zveřejnění, jsou považovány za informace INTERNÍ.	Sdílený všemi	
3	Neveřejné	Informace přístupné pouze určené skupině zaměstnanců organizace, zpravidla v rámci organizační jednotky, nebo informace poskytované určené skupině externích osob (např. členové RM a ZM). Patří sem také informace týkající se určeného nebo určitelného subjektu dle GDPR (tzv. osobní údaje). Na tyto informace se vztahují ustanovení jmenovaného nařízení. Jde především o informace vytvářené a zpracovávané v rámci výkonu veřejné správy nebo jiné činnosti organizace ve vztahu ke konkrétním subjektům (fyzickým nebo právnickým osobám).	Sdílený na OJ	
4	Chráněné	Informace, jejichž vyzrazení by mohlo závažným způsobem poškodit fungování organizace nebo její dobré jméno, poškodit zájmy subjektu osobních údajů, způsobit závažné majetkové ztráty, zapříčinit přerušení nebo zmaření významných procesů. Na tyto informace se mohou vztahovat ustanovení GDPR. Patří sem vždy typy informací, pro něž to výslovně stanovuje tato bezpečnostní politika, zvláštní kategorie osobních údajů a informace, které tak označí garant příslušného informačního aktiva. Tyto informace mohou být přístupné pouze určeným jednotlivcům nebo skupinám zaměstnanců organizace.	Utajený, Vyhrazený	

20.3 Klasifikační stupeň 3 "NEVEŘEJNÝ" je považován za výchozí stupeň klasifikace. Pokud se uživatel setká s neoznačenou informací, nakládá s ní jako s informací "NEVEŘEJNOU" do té doby, než ověří skutečnou klasifikaci informace.

20.4 Označování a zacházení s informacemi

20.4.1 Dokumenty v listinné podobě, které obsahují informace zařazené do stupně 4 "CHRÁNĚNÉ" musí být vždy viditelně označeny jedním z následujících návěští:

a) CHRÁNĚNÉ

b) TAJNÉ

c) DŮVĚRNÉ

20.4.2 Dokumenty se označují návěštím zpravidla v pravém horním rohu, u vícestránkových dokumentů minimálně na první straně.

20.4.3 Pokud je to možné, musí být zajištěno automatizované označení chráněných informací v digitální podobě před jejich výstupem do listinné podoby (např. v šabloně nebo tiskové sestavě). Pokud toto nelze zajistit, musí uživatel listinnou podobu dokumentu označit ihned po jejím vytištění.

20.4.4 Za řádné označení chráněného dokumentu v listinné podobě odpovídá uživatel, který provedl jeho vytištění.

ČÁST V.

BEZPEČNOST Z HLEDISKA LIDSKÝCH ZDROJŮ

Článek 21

Před vznikem pracovního vztahu

21.1 Role a odpovědnosti

21.1.1 Role a odpovědnosti při zpracování a využívání informací a prostředků pro zpracování informací vyplývají z Pracovní náplně zaměstnance. Za to odpovídá přímý nadřízený zaměstnance.

21.1.2 V případě externích uživatelů a dodavatelů musí být role a odpovědnosti při zpracování a využívání informací prostřednictvím ICT prostředků uvedeny ve smlouvě o ochraně informací a přístupu do datové sítě. Za uzavření této smlouvy odpovídá ředitel organizace nebo vedoucí odboru MMK, který uzavřel příslušnou dodavatelskou smlouvu.

21.2 Prověřování

21.2.1 Uchazeči o zaměstnání v organizaci musí být prověřováni v rámci personální politiky, která požaduje:

a) prověření identity uchazeče;

b) prokázání bezúhonnosti;

c) ověření správnosti údajů uvedených v životopisu, zejména dosažené vzdělání a další schopnosti.

21.2.2 Další podrobnější ověřování způsobilosti se provádí u uchazečů, kteří v rámci své pracovní činnosti přijdou do styku s chráněnými informacemi nebo budou zastávat funkce kritické pro provoz ICT systémů. V těchto případech definuje ředitel organizace nebo vedoucí příslušného odboru MMK požadavky na prověřování postojů uchazeče k informační bezpečnosti.

21.2.3 U dodavatelských firem se prověřování provádí v rámci zadávání veřejné zakázky. Předmětem prověřování jsou především kvalifikační předpoklady dle zákona o zadávání veřejných zakázek. Je-li to účelné, může být v rámci veřejné zakázky po uchazečích požadováno splnění kvalifikační předpokladů v oblasti řízení bezpečnosti informací (např. certifikace na systém řízení bezpečnosti informací dle ČSN ISO/IEC 27001, osvědčení dle GDPR).

21.2.4 V případě, že výběr dodavatele probíhá v režimu zakázky malého rozsahu a je to účelné, využije se požadavek na prokázání profesních kvalifikačních předpokladů a technických kvalifikačních předpokladů obdobně, jako by veřejná zakázka probíhala v režimu podlimitní veřejné zakázky.

21.2.5 Za prověření dodavatelských firem odpovídá správce veřejné zakázky dle Směrnice o zadávání veřejných zakázek.

21.3 Podmínky výkonu pracovní činnosti

21.3.1 Odpovědnosti zaměstnanců organizace za bezpečnost informací vyplývají z pracovněprávních předpisů[2)], vnitřních předpisů[3)] a jiných právních předpisů[4)] a povinnosti z nich vyplývající platí i mimo pracoviště a pracovní dobu zaměstnance a trvají i po ukončení pracovního poměru.

Článek 22

Během pracovního vztahu

22.1 Odpovědnosti vedoucích zaměstnanců

22.1.1 Ředitel organizace nebo tajemník MMK a vedoucí zaměstnanci v organizaci mají odpovědnost za to, že:

a) podřízení zaměstnanci byli prokazatelně seznámeni s vnitřními předpisy a zvláštními předpisy o ochraně informací a zachování mlčenlivosti ještě předtím, než jim je umožněn přístup k informacím a prostředkům pro zpracování informací,

b) jsou dostatečně motivováni dodržovat bezpečnostní politiku,

c) podřízení zaměstnanci si udržují a prohlubují své dovednosti a svou kvalifikaci pro práci s ICT prostředky.

22.2 Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací

22.2.1 Ke zvyšování povědomí v oblasti informační a kybernetické bezpečnosti a používaných informačních systémů slouží pravidelná školení a vzdělávání všech uživatelů. Za vypracování plánu vzdělávání a jeho vyhodnocení odpovídá přímý nadřízený zaměstnance.

22.2.2 Všichni zaměstnanci musí být řádně proškoleni v oblasti bezpečnostní politiky a ochrany osobních údajů. V případě nově přijatých zaměstnanců na MMK je toto školení součástí jejich adaptačního vzdělávacího programu. Za účast zaměstnance na tomto školení odpovídá jejich přímý nadřízený.

22.2.3 Ředitel organizace nebo tajemník MMK odpovídají za to, že organizace vede evidenci záznamů o školení a

požadavcích na vzdělávání v oblasti informační a kybernetické bezpečnosti.

22.3 Disciplinární řízení

22.3.1 Každé zjištění porušení bezpečnostní politiky ze strany zaměstnance musí být řešeno v rámci disciplinárního řízení. Vedením disciplinárního řízení je pověřena komise, kterou tvoří ředitel organizace nebo tajemník MMK, přímý nadřízený zaměstnance, pověřenec a bezpečnostní správce.

d)
(dále jen "disciplinární komise").

22.3.2 Disciplinární komise může na své jednání přizvat další osoby, zejména systémového inženýra, správce ICT, lokálního administrátora nebo personalistu.

22.3.3 Disciplinární komise rozhoduje o míře závažnosti porušení bezpečnostní politiky zaměstnancem. Přitom bere v potaz, zda se jednalo porušení úmyslné nebo neúmyslné, jeho rozsah, důsledky a zda došlo k porušení ochrany osobních údajů nebo informací klasifikovaných stupněm 4 "CHRÁNĚNÉ".

22.3.4 V případě zjištění závažného porušení bezpečnostní politiky zaměstnancem nebo v případě, kdy je oprávněná obava z pokračování v porušování bezpečnostní politiky může být zaměstnanec okamžitě zbaven přístupových práv nebo i přístupu k aktivům organizace.

22.3.5 Rozhodnutí o míře a způsobu potrestání zaměstnance je v kompetenci ředitele organizace nebo tajemníka MMK.

22.3.6 Podnět k vedení disciplinárního řízení se zaměstnancem pro porušení bezpečnostní politiky může podat pověřenec nebo bezpečnostní správce na základě ohlášené bezpečnostní události nebo bezpečnostního incidentu.

Článek 23

Ukončení nebo změna pracovního vztahu

23.1 Odpovědnosti při ukončení pracovního vztahu

23.1.1 V případě ukončení pracovního vztahu se zaměstnancem musí být zajištěny následující úkony:

	Úkon	Odpovídá	Technicky zajišťuje
1.	Odebrání přístupových práv do informačních systémů	nadřízený zaměstnance	správce aplikací
2.	Zrušení uživatelského účtu pro přístup do datové sítě		správce datové sítě
3.	Navrácení zapůjčených HW prostředků.		správce majetku
4.	Navrácení zapůjčených autentizačních zařízení (čipových karet apod.).		ten kdo zařízení vydal
5.	Zneplatnění zaměstnaneckých kvalifikovaných a komerčních certifikátů.		operátor CA

23.1.2 Všechny úkony musí být provedeny nejpozději ke dni skončení pracovního poměru zaměstnance. Provedení jednotlivých úkonů musí být potvrzeno ve výstupním listu zaměstnance. Ředitel organizace nebo tajemník MMK odpovídají za to, že jsou evidovány výstupní listy zaměstnanců. Na MMK vede evidenci oddělení lidských zdrojů MMK. Na MPK vede evidenci úsek lidských zdrojů a poplatků MPK.

23.2 Odpovědnosti při změně pracovního vztahu

23.2.1 V případě změny pracovního vztahu (např. změna pracovní pozice nebo pracovní role zaměstnance) musí být přezkoumán rozsah přístupových oprávnění. Za přezkoumání a aktualizaci rozsahu přístupových práv odpovídá přímý nadřízený zaměstnance, do jehož útvaru zaměstnanec přechází. Nejpozději ke dni účinnosti změny pracovního zařazení zaměstnance je přímý nadřízený povinen podat aktualizovanou žádost o nastavení nebo zrušení přístupových práv Správci ICT.

23.2.2 Pokud mají být zaměstnanci po omezenou dobu ponechána přístupová oprávnění k informacím a informačním systémům vázaných na původní pracovní pozici nebo roli, může tak být učiněno pouze se souhlasem nadřízeného, z jehož útvaru zaměstnanec přechází.

ČÁST VI.

ŘÍZENÍ PŘÍSTUPU

Článek 24

Požadavky na řízení přístupu

24.1 Přístup k ICT prostředkům a informacím musí být řízen na základě provozních potřeb a bezpečnostních požadavků. Za určení rozsahu přístupových práv interního uživatele odpovídá jeho přímý nadřízený.

24.2 Politika řízení přístupu a pravidla schvalování přístupů k ICT prostředkům pro jednotlivé skupiny uživatelů jsou popsány v Celkové bezpečnostní politice informací, Bezpečnostní směrnici pro externí uživatele, Bezpečnostní směrnici pro dodavatele a Provozní a bezpečnostní směrnici Technologického centra Karviná. Za politiku řízení přístupu a její pravidelné přezkoumávání odpovídá bezpečnostní správce.

Článek 25

Řízení přístupu uživatelů

25.1 Přístup k ICT prostředkům a informacím mohou uživatelé získat pouze na základě předchozího schválení a pouze ve schváleném rozsahu. Za správné nastavení ICT prostředků, evidenci schválených rozsahů oprávnění a evidenci skutečného nastavení oprávnění odpovídá správce ICT. Bezpečnostní správce je oprávněn kdykoliv provést kontrolu souladu evidenčního stavu se skutečným nastavením rozsahu oprávnění jednotlivých prostředků pro zpracování informací.

25.2 Pro přístup k ICT prostředkům se využívají přístupové účty, které jednoznačně definují uživatele, jeho pracovní prostředí a sadu oprávnění k prostředku pro zpracování informací. Přístupový účet je vždy definován jednoznačným identifikátorem (uživatelským jménem). Použití přístupového účtu je vždy podmíněno některou z forem autentizace uživatele:

a) přístupovým heslem,

b) kryptografickým prostředkem (např. certifikátem),

c) biometrickým údajem.

25.3 Registrace uživatele

25.3.1 Pro přístup uživatele k ICT prostředkům jsou zřizovány tzv. uživatelské účty. Uživatelský účet je vyhrazen pro přístup osoby, které byl zřízen - vlastník uživatelského účtu. Použití uživatelského účtu jinou osobou je výslovně zakázáno.

25.3.2 Ve zvláštních případech mohou být zřizovány skupinové účty pro přístup více uživatelů. Každý skupinový účet má určen vlastníka skupinového účtu. Zřízení skupinového účtu musí být předem schváleno bezpečnostním správcem ICT.

25.4 Řízení privilegovaného přístupu

25.4.1 Pro privilegovaný přístup k ICT prostředkům zvláštního významu, jako jsou serverové systémy, systémy pro správu aplikací apod., jsou zřizovány administrátorské účty. Administrátorský účet je vyhrazen pro přístup osoby, které byl zřízen - vlastník administrátorského účtu. Použití administrátorského účtu jinou osobou je výslovně zakázáno. Zřízení administrátorského účtu musí být předem schváleno bezpečnostním správcem. Administrátorské účty smí být využívány pouze pro správu systému a nesmí být využívány pro běžnou uživatelskou práci.

25.4.2 Pro zajištění provozu ICT prostředků jsou zřizovány systémové účty. Jedná se o zvláštní typ uživatelského účtu, který slouží pro automatizovaný přístup aplikací k serverovým službám a není určen k použití uživateli ani administrátory. Vlastníkem systémových účtů je vždy správce příslušného prostředku pro zpracování informací. Zřízení systémového účtu schvaluje systémový inženýr.

25.5 Správa uživatelských hesel

25.5.1 V případě, že autentizačním údajem k uživatelskému účtu, skupinovému účtu nebo administrátorskému účtu je přístupové heslo, pak je k takovému účtu generováno jednorázové přístupové heslo, které musí být při prvním přihlášení vlastníkem účtu změněno. Generování, správu a předávání jednorázových přístupových hesel provádí správce ICT. Jednorázová přístupová hesla ani následná hesla pro tyto typy účtů se neevidují.

25.5.2 Přístupová hesla k systémovým účtům generuje správce příslušného prostředku pro zpracování informací a vede jejich evidenci. Evidence přístupových hesel k systémovým účtům je klasifikována stupněm "CHRÁNĚNÉ" a musí být bezpečně uložena u bezpečnostního správce. Hesla se ukládají do samostatných obálek označených názvem systémového účtu, jménem odpovědného správce a datem uložení. Obálky musí být zalepeny a zabezpečeny tak, aby jejich obsah nebylo možné vyjmout bez porušení. Součástí zabezpečení obálky je vždy podpis odpovědného správce a razítko a podpis bezpečnostního správce. K evidenci přístupových hesel systémových účtů smí získat přístup pouze příslušný správce prostředku pro zpracování informací, bezpečnostní správce, systémový inženýr a ředitel organizace nebo tajemník MMK.

25.6 Používání přístupových hesel

25.6.1 Hesla ke všem typům přístupových účtů jsou klasifikována stupněm "CHRÁNĚNÉ". Heslo k přístupovému účtu smí znát pouze vlastník účtu, v případě skupinového nebo systémového účtu také vlastníkem určené osoby.

25.7 Politika přístupových hesel

25.7.1 Pro přístupová hesla k uživatelským a skupinovým účtům jsou stanoveny následující požadavky na jejich kvalitu:

a) Minimální délka: 8 znaků

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

c) Minimální platnost: 5 dnů

d) Maximální platnost: 1 rok

e) Historie: 5

25.7.2 Pro přístupová hesla k administrátorským účtům jsou stanoveny následující požadavky na jejich kvalitu:

a) Minimální délka: 12 znaků

b) Minimální složitost (komplexita): alespoň tři ze skupin: velká písmena, malá písmena, číslice, zvláštní znaky (např. / * , . ? %)

c) Minimální platnost: 30 dnů

d) Maximální platnost: 1 rok

e) Historie: 5

25.7.3 Pro přístupová hesla k systémovým účtům jsou stanoveny následující požadavky na jejich kvalitu:

a) Minimální délka: 10 znaků

b) Minimální složitost (komplexita): alespoň tři ze skupin: velká písmena, malá písmena, číslice, zvláštní znaky (výčet)

c) Minimální platnost: není určena

d) Maximální platnost: není určena

e) Historie: 5

25.8 Přezkoumání přístupových práv uživatelů

25.8.1 Přístupová práva uživatelů musí být přezkoumána a aktualizována vždy při přeřazení uživatele na jinou pracovní pozici. Za přezkoumání a aktualizaci odpovídá přímý nadřízený přeřazeného uživatele. Pokud při přeřazení dochází ke změně přímého nadřízeného, odpovídá za přezkoumání a aktualizaci ten nadřízený, do jehož útvaru uživatel přechází.

25.8.2 Přístupová práva privilegovaných uživatelských účtů musí být přezkoumána a aktualizována minimálně 1x ročně. Za přezkoumání a aktualizaci administrátorských účtů odpovídá bezpečnostní správce. Za přezkoumání a aktualizaci systémových účtů odpovídá příslušný správce prostředků pro zpracování informací.

Článek 26

Mobilní zařízení a práce na dálku

26.1 Mobilní zařízení představují vyšší stupeň rizika z hlediska ochrany informací a ICT prostředků. Pro jejich ochranu proto platí zvláštní opatření (viz Článek 32 a Článek 42).

ČÁST VII.

PRAVIDLA PRO UŽIVATELSKÉ ÚČTY

Článek 27

Zřizování, změna a rušení uživatelských účtů

27.1 Uživatelský účet pro přístup do datové sítě organizace může být zřízen pouze na dobu trvání pracovního nebo obdobného poměru u zaměstnanců nebo na dobu výkonu funkce primátora nebo náměstka nebo na dobu trvání mandátu zastupitele. Rekvalifikantům nebo praktikantům může být zřízen uživatelský účet pouze, pokud jejich praxe nebo rekvalifikace trvá alespoň 3 měsíce.

27.2 Vytváření nového uživatelského účtu, jeho změny nebo zrušení a nastavování rozsahu přístupových práv se provádí na základě žádosti o nastavení přístupových práv podané bezpečnostnímu správci.

27.3 Podání a schvalování žádostí:

a) žádosti pro uživatelské účty zaměstnanců schvaluje a podává jejich nadřízený zaměstnanec,

b) žádosti pro uživatelské účty vedoucích odborů MMK, primátora a náměstků schvaluje a podává tajemník MMK,

c) žádosti pro uživatelský účet ředitele organizace nebo tajemníka MMK schvaluje a podává primátor.

27.4 Ten kdo žádost schvaluje a podává, odpovídá za to, že rozsah přístupových oprávnění odpovídá náplni práce příslušného uživatele a potřebám jeho pracovní činnosti nebo výkonu jeho funkce.

27.5 Všechny žádosti formálně schvaluje také bezpečnostní správce. Ten odpovídá za to, že žádost obsahuje veškeré náležitosti a byla podána v souladu s bezpečnostní politikou.

27.6 Podávání a schvalování žádostí se řídí podle následující matice:

Uživatelský účet	Žádost podává a schvaluje	Žádost formálně schvaluje
zaměstnance organizace	nadřízený zaměstnance	bezpečnostní správce
vedoucího odboru MMK	tajemník MMK	
vedoucího zaměstnance MPK	ředitel MPK	
tajemníka MMK	primátor	
ředitele organizace	primátor	
primátora a náměstků	tajemník MMK	

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

27.8 Uživatelský účet může být dočasně blokován (např. z důvodu dlouhodobé nemoci, podezření na porušení bezpečnostní politiky apod.). Blokování uživatelských účtů se řídí následujícími pravidly:

a) Žádost o blokování uživatelského účtu se schvaluje a podává obdobně jako žádost o jeho zřízení, změnu nebo zrušení.

b) Blokování uživatelského účtu může nařídit kdykoliv bezpečnostní správce nebo pověřenec z důvodu odůvodněného podezření na zneužití uživatelského účtu nebo v oprávněném zájmu zachování informační a kybernetické bezpečnosti. O blokování uživatelského účtu a jeho důvodech bezpečnostní správce bezodkladně informuje příslušeného uživatele a jeho nadřízeného zaměstnance.

c) Blokování uživatelského účtu může provést kdykoliv správce ICT z důvodu odůvodněného podezření na zneužití uživatelského účtu nebo v oprávněném zájmu zachování informační a kybernetické bezpečnosti. O blokování účtu a jeho důvodech správce ICT bezodkladně informuje příslušeného uživatele, jeho nadřízeného zaměstnance a bezpečnostního správce.

d) O provedených blokacích uživatelských účtů provádí bezpečnostní správce záznam do evidence bezpečnostních incidentů.

Článek 28

Ochrana uživatelských účtů a politika hesel

28.1 Uživatelský účet smí používat pouze osoba, pro kterou byl zřízen.

28.2 Identifikační údaje k uživatelskému účtu, zejména přístupové heslo nebo jiné autentizační prostředky, musí uživatel chránit a nesmí je poskytovat žádným dalším osobám.

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

28.4 Uživatel nesmí umožnit žádné další osobě pracovat s ICT prostředky prostřednictvím svého uživatelského účtu. Výjimkou z tohoto pravidla je poskytování vzdálené pomoci správcem ICT v souladu s článkem Článek 54.

28.5 V případě podezření na vyzrazení hesla je uživatel povinen neprodleně své heslo změnit. Zároveň tuto skutečnost musí uživatel nahlásit jako bezpečnostní událost dle odst. 56.1.

28.6 Požadavky na kvalitu přístupového hesla jsou stanoveny v odst. 25.7.

Článek 29

Ochrana certifikátů

29.1 Pro účely autentizace, autorizace a zajištění důvěry v některých prostředcích pro zpracování informací jsou využívány certifikáty veřejných certifikačních autorit (dále jen "veřejné certifikáty"). Veřejné certifikáty jsou vydávány ve variantách:

a) Kvalifikované certifikáty pro kvalifikovaný elektronický podpis - slouží k digitálnímu podepisování (autorizaci) elektronických úkonů, dále také "podpisový certifikát",

b) komerční certifikáty - slouží k přihlašování (identifikaci) do informačních systémů, dále také "přihlašovací certifikát".

c) Systémové certifikáty - slouží k zajištění důvěry při komunikaci mezi prostředky ICT.

29.2 Certifikáty pro vytváření kvalifikovaného elektronického podpisu (dle zák. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce) se ukládají na USB token nebo čipovou kartu a jsou chráněny PIN kódem. Ostatní certifikáty mohou být ukládány i na jiná úložiště.

29.3 Hesla a PIN kódy k USB tokenům, čipovým kartám a certifikátům jsou klasifikována jako "CHRÁNĚNÁ" a uživatel je nesmí nikomu sdělit. Pro jejich ochranu platí stejná pravidla, jako pro ochranu identifikačních údajů uživatelského účtu.

29.4 Uživatel je povinen chránit čipové karty nebo jiné prostředky pro autentizaci před odcizením, ztrátou nebo zneužitím. Ztrátu nebo zcizení čipové karty nebo jiného prostředku pro autentizaci musí uživatel nahlásit jako bezpečnostní událost dle odst. 56.1.

29.5 Za veškeré úkony provedené veřejným certifikátem nese plnou odpovědnost uživatel, na jehož jméno byl veřejný certifikát vydán.

ČÁST VIII.

PRAVIDLA PRO POUŽÍVÁNÍ ICT PROSTŘEDKŮ

Článek 30

Společná pravidla pro používání ICT prostředků

30.1 ICT prostředky se rozumí veškeré programové a technické vybavení, které je provozováno za účelem zpracování a ukládání informací. Patří sem zejména počítače, notebooky, tiskárny, skenery, tablety, chytré mobilní telefony a další počítačové příslušenství (dále také "zařízení") a jejich programové vybavení.

30.2 Každý uživatel je povinen seznámit se a dodržovat návody na použití, metodické nebo jiné návody určující podmínky provozu daného ICT prostředku (tzv. provozní dokumentace).

30.3 Uživatel nesmí:

a) instalovat a používat neschválené soukromé ICT prostředky v datové síti organizace,

b) demontovat nebo zaměňovat komponenty jednotlivých zařízení,

c) odpojovat a přemisťovat pevně instalovaná zařízení bez svolení správce majetku,

d) používat soukromá výměnná úložiště dat (např. CD-ROM, flash disky apod.) pro ukládání pracovních dat klasifikovaných vyšším stupněm než "veřejné",

e) měnit systémové nastavení ICT prostředků,

f) umožnit neoprávněný přístup k ICT prostředkům.

Článek 31

Společná pravidla běžné údržby a péče o zařízení

31.1 Uživatel musí udržovat povrch zařízení čistý a nepoškozený. Uživatel smí provádět povrchové čistění zařízení za pomocí čistého suchého měkkého hadříku nebo speciálního vlhčeného ubrousku, určeného pro ICT zařízení.

31.2 Uživatel musí dbát zvýšené opatrnosti před poškozením zařízení vodou nebo jinými tekutinami. V případě, že se zařízení dostane do styku s tekutinami, je uživatel povinen neprodleně vhodným způsobem zamezit dalšímu rozšíření nebo průniku tekutiny dovnitř zařízení a odpojit zařízení od zdroje elektrického proudu. Tuto událost musí nahlásit jako bezpečnostní událost dle odst. 56.1.

Článek 32

Specifická pravidla pro mobilní zařízení

32.1 Mobilním zařízením se rozumí zejména notebooky, tablety, mobilní telefony a chytré telefony (smart phone).

32.2 Za fyzickou ochranu mobilního zařízení a ochranu dat v nich uložených odpovídá uživatel, kterému bylo svěřeno k užívání.

32.3 Uživatel musí zajistit zejména, aby nemohlo být mobilní zařízení poškozeno, zničeno, ztraceno, zcizeno nebo použito jinou neoprávněnou osobou. Stejné požadavky ochrany platí pro data v něm uložená.

32.4 Uživatel nesmí nechat nezabezpečené mobilní zařízení bez dozoru.

32.5 Uživatel nesmí zapůjčit nebo jinak zpřístupnit mobilní zařízení jiné neoprávněné osobě.

32.6 Zcizení, ztrátu nebo neoprávněné použití mobilního zařízení musí uživatel nahlásit jako bezpečnostní událost dle odst. 56.1.

Článek 33

Specifická pravidla pro tisková zařízení

33.1 Tiskovým zařízením se rozumí zejména tiskárny, kopírky, plotry a kombinovaná (tzv. multifunkční) zařízení s funkcí tisku.

33.2 Uživatel smí využívat tisková zařízení pouze pro pracovní účely. Tisk soukromých výstupů je zakázán.

33.3 Uživatel je povinen zabezpečit, že tiskové výstupy obsahující data klasifikována stupněm vyšším než "VEŘEJNÉ" nebudou volně přístupné neoprávněným osobám.

33.4 Zcizení nebo ztrátu "neveřejných" tiskových výstupů musí uživatel nahlásit jako bezpečnostní incident dle odst. 56.1.

Článek 34

Specifická pravidla pro skenovací zařízení

34.1 Skenovacím zařízením se zejména samostatné skenery, kopírky a kombinovaná (tzv. multifunkční) zařízení s funkcí skenování.

34.2 Uživatel nesmí nechávat ve skenovacích zařízeních předlohy obsahující data klasifikována stupněm vyšším než "VEŘEJNÉ".

34.3 Zcizení nebo ztrátu "neveřejných" tiskových předloh musí uživatel nahlásit jako bezpečnostní incident dle odst. 56.1.

Článek 35

Specifická pravidla pro ostatní zařízení

35.1 Ostatním zařízením se rozumí jakékoliv jiné zařízení se schopností zpracovávat informace bez ohledu na jejich formu (např. obrazové, zvukové aj.). Patří sem zejména fotoaparáty, kamery, diktafony a jiná záznamová zařízení.

35.2 Uživatel je povinen zabezpečit, že ostatní zařízení obsahující data klasifikována stupněm vyšším než "VEŘEJNÉ" nebudou volně přístupné neoprávněným osobám.

35.3 Zcizení nebo ztrátu ostatních zařízení nebo dat v nich uložených musí uživatel nahlásit jako bezpečnostní incident dle odst. 56.1.

Článek 36

Používání ICT prostředků pro soukromé účely

36.1 Pokud to není výslovně zakázáno, uživatel smí využívat ICT prostředky pro soukromé účely, pokud:

a) tím neporušuje pracovní řád (zejména dodržování pracovní doby),

b) tím nevzniknou organizaci žádné přímé nebo nepřímé finanční náklady (např. za tisk, mobilní hlasové a datové služby apod.),

c) tím uživatel neomezí provoz jiných ICT zařízení v datové síti organizace (např. značným datovým tokem apod.),

d) tím uživatel nepáchá trestnou činnost (např. stahování nelegálního obsahu apod.),

e) uživatel dodržuje bezpečnostní politiku.

36.2 Uživatel smí užívat kvalifikovaný zaměstnanecký certifikát pro vytváření zaručeného elektronického podpisu nebo kvalifikovaného elektronického podpisu pro soukromé účely, pokud

a) je jednoznačně patrné, že úkon provedený tímto certifikátem učinil jako soukromá osoba,

b) tím neporušuje zákony nebo jiné právní předpisy České republiky nebo jiného státu uznaného Českou republikou,

c) tím nejedná proti zájmům organizace nebo SMK a nepoškozuje dobré jméno organizace nebo SMK.

ČÁST IX.

PRAVIDLA PRO POUŽÍVÁNÍ DATOVÉ SÍTĚ

Článek 37

Provoz datové sítě

37.1 Datová síť organizace je v provozu 24 hodin denně s odstávkami pro zajištění její nutné údržby. O plánovaných omezeních a odstávkách v provozu datové sítě nebo informačních systémů jsou uživatelé předem vyrozuměni správcem ICT prostřednictvím e-mailu.

37.2 Uživatel je povinen dbát všech pokynů správce ICT v souvislosti s provozem datové sítě a informačních systémů. Pokyny zasílané e-mailem musí být důvěryhodné dle odst. 40.7 a nesmí být v rozporu s bezpečnostní politikou. V případě, že pokyny nesplňují požadavky na důvěryhodnost a soulad s bezpečnostní politikou, uživatel se těmito pokyny neřídí a o přijetí takových pokynů bezodkladně informuje bezpečnostního správce.

Článek 38

Podmínky přístupu do datové sítě

38.1 Uživatel je oprávněn k přístupu do datové sítě pouze prostřednictvím jemu zřízeného uživatelského účtu.

38.2 Uživatel v žádném případě nesmí využívat pro přístup do datové sítě a k informačním systémům uživatelský účet jiné osoby.

Článek 39

Používání internetu

39.1 Všichni uživatelé mají umožněn přístup k internetu. Přístup k internetu je vázán na uživatelský účet.

39.2 Uživatel při využívání internetu nesmí navštěvovat internetové stránky s nevhodným obsahem, zejména:

a) stránky obsahující pornografii,

b) stránky zobrazující násilí,

c) stránky podněcující k rasismu,

d) stránky nabízející nelegální software,

e) stránky, jejichž obsah je jinak v rozporu s platnými zákony.

Správce ICT je oprávněn technickými prostředky blokovat obsah webových stránek spadajících do výše uvedených kategorií a to na základě automatizovaného vyhodnocení tzv. webovým filtrem.

39.3 Uživatel si musí být vědom, že využívání internetu je monitorováno za účelem udržení stanovené úrovně bezpečnosti, technické údržby, řešení technických problémů apod. Zejména jsou monitorovány a ukládány URL adresy stránek, na něž uživatel přistupoval, případně jejich názvy nebo celý obsah těchto stránek.

39.4 Uživatel smí využívat přístup k internetu pro soukromé účely v souladu s odst. 36.1. Při využívání internetu pro soukromé účely platí všechna omezení bezpečnostní politiky, zejména ustanovení odst. 39.1 až 39.3.

Článek 40

Používání elektronické pošty

40.1 Všichni uživatelé mají zřízenu jednu e-mailovou schránku v doméně organizace. Kapacita e-mailové schránky na serveru je pro každého uživatele omezena. Z důvodů omezené velikosti schránek uživatelů je každý uživatel povinen průběžně udržovat svou e-mailovou schránku, zejména:

a) pravidelně stahovat nové zprávy z poštovního serveru (pokud tomu nebrání jiné okolnosti, musí mít uživatel trvale zapnutý mail),

b) pravidelně mazat staré (nepotřebné) e-maily,

c) pravidelně archivovat e-maily, jež nejsou aktuální, ale je nutné je uchovat,

d) pravidelně odstraňovat e-maily přesouvané do složky "Odstraněná pošta".

40.2 Uživatel (vlastník poštovní schránky) je odpovědný za průběžné vyřizování e-mailové korespondence.

40.3 Z důvodů nebezpečí napadení škodlivým kódem je přísně zakázáno otevírat a spouštět jakékoliv neověřené připojené soubory nebo aktivní odkazy, zejména od neznámých odesílatelů. To neplatí pro přílohy a aktivní odkazy zaslané správcem ICT, pokud je jeho e-mail důvěryhodný dle odst. 40.7.

40.4 Uživatel nesmí používat elektronickou poštu k rozesílání nevyžádané pošty (tzv. SPAM zásilek).

40.5 V případě plánované nepřítomnosti musí uživatel nastavit automatické odpovědi na doručené zásilky s uvedením plánované doby nepřítomnosti a jména osoby, která jej zastupuje.

40.6 Veškerá e-mailová komunikace odcházející od uživatele musí být opatřena textovým podpisem s případným logem a kontaktními údaji dle platného vzoru organizace.

40.7 E-mailové zprávy zasílané správcem ICT jsou navíc opatřovány kvalifikovaným elektronickým podpisem pro zajištění důvěryhodnosti odesílané zprávy. Zprávy, které nejsou elektronickým podpisem opatřeny, jsou považovány za nedůvěryhodné a uživatelé jsou povinni pravost takové zprávy ověřit.

Článek 41

Používání bezdrátových sítí

41.1 V organizaci mohou být provozovány bezdrátové (WiFi) sítě pro účely připojování interních uživatelů, externích uživatelů, dodavatelů a klientů.

41.2 Bezdrátové sítě pro připojování interních uživatelů musí být konfigurovány tak, aby byl zabezpečen šifrovaný provoz v této síti a připojení do této sítě pouze po ověření klienta minimálně na úrovni algoritmu WPA2.

41.3 Veřejné bezdrátové sítě pro připojování klientů musí být konfigurovány tak, aby byly odděleny od provozu vnitřní datové sítě organizace a byl znemožněn přístup uživatele k jiným aktivům organizace. Přístup k těmto sítím je umožněn na základě souhlasu s provozním řádem veřejné bezdrátové sítě. V těchto sítích je umožněn přístup pouze k prostředkům v síti Internet.

41.4 Přístupové údaje k bezdrátovým sítím dle odst. 42.2 jsou klasifikovány jako "CHRÁNĚNÉ" a nesmí být poskytovány jiným osobám.

41.5 Za plnění bezpečnostních opatření dle odst. 42.2 a 42.3 odpovídá příslušný správce ICT.

41.6 Vydáváním provozního řádu veřejné bezdrátové sítě provozované SMK je pověřen Odbor organizační MMK.

Článek 42

Práce na dálku

42.1 Uživatel smí přistupovat vzdáleně do datové sítě organizace pouze v rámci plnění pracovních úkolů.

42.2 Uživatel odpovídá za ochranu informací a ICT prostředků při využívání vzdáleného přístupu stejně, jako při přístupu z datové sítě organizace. Platí pro něj proto všechna ustanovení bezpečnostní politiky.

42.3 Pro vzdálený přístup je zakázáno používat veřejná nebo jiná neznámá zařízení, která nejsou pod kontrolou uživatele (např. veřejných nebo cizích zařízení). U těchto zařízení je vysoké riziko napadení škodlivým kódem.

42.4 Uživatel odpovídá za to, že v zařízení, které využívá pro vzdálený přístup, nebudou ukládány v nezašifrované podobě žádné informace s klasifikací vyšší než "veřejné". Ukládání neveřejných informací do soukromých zařízení v jakékoliv podobě je výslovně zakázáno.

42.5 Uživatel využívající vzdálený přístup do datové sítě musí zajistit bezpečnost a ochranu prostředí, z něhož vzdáleně přistupuje. Zejména je povinen zajistit, že

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

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

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

42.6 Vzdálené připojení k virtuálnímu počítači

42.6.1 Uživatelé virtuálních počítačů se mohou připojovat ke svému virtuálnímu počítači ze sítě Internet na adrese https://virtual.karvina.cz nebo prostřednictvím aplikace VMware Horizon View za těchto podmínek:

a) v zařízení je instalována aplikace VMware Horizon View z oficiálního zdroje; za oficiální zdroje se považují:
i) adresa virtual.karvina.cz, pro prostředí Microsoft Windows,
ii) úložiště Google Play, pro prostředí Android,
iii) úložiště iTunes, pro prostředí iOS,
iv) úložiště Windows Phone Store, pro prostředí Windows Phone.

b) adresa pro připojení je virtual.karvina.cz.

ČÁST X.

PRAVIDLA PRO NAKLÁDÁNÍ S INFORMACEMI

Článek 43

Datová úložiště

43.1 Uživatelé mohou využívat pro ukládání informací tyto typy datových úložišť:

a) lokální disky běžného počítače, virtuálního počítače nebo notebooku (velikost úložiště je omezena kapacitou lokálních disků, data těchto disků nejsou automatizovaně zálohována a za jejich případné zálohování odpovídá uživatel),

b) síťová úložiště v datové síti organizace,

c) privátní cloudová úložiště mimo datovou síť organizace; jedná se o úložiště vyhrazená pro danou organizaci poskytovatelem cloudových služeb na základě řádně uzavřené smlouvy,

d) veřejná cloudová úložiště mimo datovou síť organizace; jedná se o úložiště veřejných poskytovatelů cloudových služeb (např. uschovna.cz aj.).

43.2 Uživatel nesmí ukládat na žádná datová úložiště svá soukromá data.

43.3 Uživatel nesmí ukládat na veřejná cloudová úložiště informace klasifikované vyšším stupněm než "VEŘEJNÉ".

43.4 Informace klasifikované stupněm "NEVEŘEJNÉ" nebo "CHRÁNĚNÉ" smí uživatel ukládat v mobilních zařízeních výhradně na úložiště s funkcí šifrování.

43.5 Uživatel si musí být vědom, že obsah veškerých úložišť je monitorován a může být přístupný jeho nadřízenému, správci ICT a případně i dalším osobám na základě schváleného přístupu a to i bez jeho souhlasu.

43.6 Uživatel musí hospodárně využívat kapacitu všech úložišť, tzn. především mazat nepotřebné soubory.

Článek 44

Výměnná úložiště

44.1 Výměnnými úložišti se rozumí veškerá zařízení sloužící k ukládání dat, která nejsou pevně zabudována v počítači nebo jiném mobilním zařízení. Mezi výměnná úložiště patří zejména USB disky (přenosné disky, flash disky), paměťové karty, média CD-ROM a DVD-ROM, diskety apod.

44.2 Uživatel smí na výměnná média ukládat informace klasifikované vyšším stupněm než "VEŘEJNÉ", pouze v souvislosti s plněním pracovních povinností.

44.3 Informace klasifikované stupněm "NEVEŘEJNÉ" nebo "CHRÁNĚNÉ" smí uživatel ukládat výhradně na řádně označená a evidovaná výměnná úložiště s funkcí šifrování. Označováním, evidencí a výdejem těchto úložišť je pověřen správce ICT.

44.4 Ztrátu nebo zcizení jakéhokoliv výměnného úložiště je uživatel povinen nahlásit jako bezpečnostní incident dle odst. 56.1.

Článek 45

Ochrana dat a informací

45.1 Uživatel musí s daty a informacemi zacházet dle stupně jejich klasifikace, která je definována v Celkové bezpečnostní politice informací. Uživatel musí znát stupeň klasifikace informací zpracovávaných v informačních systémech a podle toho s nimi zacházet. Stupeň klasifikace těchto informací je uveden v evidenci informačních aktiv, která je přílohou Informační koncepce SMK.

45.2 Dokumenty obsahující informace, které jsou klasifikovány stupněm "CHRÁNĚNÉ" musí uživatel označovat v souladu s odst. 20.4.

45.3 Nepotřebné informace v jakékoliv formě (tištěné dokumenty, elektronické nosiče dat), u nichž nevznikla zákonná povinnost jejich další archivace, musí uživatel zničit (skartovat). Skartací dat se rozumí jejich smazání z datových úložišť nebo informačního systému. Skartací tisových výstupů a výměnných médií (CD-ROM DVD, diskety apod.) se rozumí jejich fyzické

zničení např. ve skartovacím stroji.

45.4 Uživatel nesmí poskytovat elektronickou poštou, uložením na datové nosiče nebo tiskem jakékoliv datové soubory jiným osobám nebo jim jakkoliv sdělovat informace získané z informačních systémů organizace. Datové soubory a informace může uživatel poskytovat pouze v rámci plnění svých pracovních povinností. Datové soubory a informace klasifikované jako "VEŘEJNÉ" může uživatel poskytovat bez omezení.

45.5 Uživatel musí zajistit, že při poskytování informací, jejich ukládání nebo tisku nebude ohrožena jejich důvěrnost.

Článek 46

Ochrana osobních údajů

46.1 Organizace je správcem osobních údajů dle GDPR.

46.2 Osobní údaje v organizaci jsou shromažďovány, uchovávány a dále zpracovávány pouze:

a) na základě souhlasu subjektu údajů,

b) pro uplatnění práv a povinností při plnění smlouvy se subjektem údajů,

c) při plnění právní povinnosti správce,

d) pro ochranu životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby,

e) při plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci,

f) pro účely oprávněných zájmů správce či třetí strany.
(dále jen "zpracování osobních údajů")

46.3 Záznamy o činnostech zpracování osobních údajů dle čl. 30 GDPR jsou součástí evidence informačních aktiv. Za správnost jejich vyplnění odpovídá garant aktiva. Garant informačního aktiva je také garantem zpracování osobních údajů.

46.4 V případě, že ke zpracování osobních údajů je potřebný souhlas subjektu údajů, odpovídá za jejich získávání a způsob jejich evidence garant zpracování osobních údajů. Ten také odpovídá za splnění informační povinnosti správce vůči subjektu údajů.

46.5 Pokud jsou součástí zpracování osobních údajů také zvláštní kategorie osobních údajů, odpovídá garant zpracování osobních údajů za to, že jsou tyto údaje zpracovávány oprávněně.

46.6 Povinnosti při zabezpečení osobních údajů jsou v této bezpečnostní politice řešeny společně pro všechna informační aktiva.

46.7 Zpracováním osobních údajů může být pověřen jiný subjekt, dále jen "zpracovatel". Zpracovatelem je vždy uživatel dle odst. 10.9.1 písm. i). Pokud zmocnění nevyplývá z jiného právního předpisu, uzavírá se s těmito uživateli Dohoda o ochraně informací a přístupu do datové sítě, která má náležitosti smlouvy o zpracování osobních údajů dle čl. 28, odst. 3 GDPR. Dohodu se zpracovatelem na MMK uzavírá Odbor organizační a za její uzavření odpovídá garant zpracování osobních údajů.

46.8 Pokud pomine důvod pro zpracování osobních údajů, musí být osobní údaje zlikvidovány (bezpečně skartovány ve všech podobách a výskytech). Další uchovávání osobních údajů je možné pouze pro potřeby archivnictví v souladu s příslušnými právními předpisy[5)]. Za likvidaci osobních údajů odpovídá garant zpracování osobních údajů.

46.9 Kontaktním místem pro uplatňování a vyřizování práv subjektů údajů je pověřenec. Příjemce žádosti o uplatnění práva subjektu údajů ji bezodkladně předá pověřenci, který si dle obsahu žádosti vyžádá součinnost příslušných garantů zpracování osobních údajů. Garanti jsou povinni spolupracovat s pověřencem a poskytnout mu nezbytnou součinnost.

46.10 Ostatní povinnosti pro nakládání s osobními údaji vyplývající z GDPR platí pro všechny uživatele, kterým byl umožněn přístup k informačním aktivům organizace.

Článek 47

Zálohování dat

47.1 Za ochranu dat před ztrátou nebo zničením na běžném počítači, virtuálním počítači nebo notebooku (lokální disky) odpovídá uživatel. Uživatel odpovídá zejména za to, že důležité informace jsou zálohovány současným uložením na jiné úložiště, než jsou lokální disky počítače nebo notebooku a tyto zálohy jsou aktuální.

47.2 Za ochranu dat před ztrátou nebo zničením na síťových úložištích odpovídá správce ICT v rámci stanoveného plánu zálohování. Uživatel si musí být vědom, že zálohování dat na síťových úložištích není prováděno kontinuálně a data z těchto úložišť jsou zálohována zpravidla 1x denně po pracovní době. Data, která byla opakovaně změněna nebo smazána před provedením zálohy, není proto možné obnovit.

Článek 48

Licenční čistota

48.1 Uživatel si musí být vědom, že programové vybavení (software) může být předmětem ochrany duševního vlastnictví podle zákona č. 121/2000 Sb., autorský zákon.

48.2 Uživatel nesmí instalovat ani používat nelegální nebo neschválený software.

48.3 Za případné trestněprávní důsledky, které vyplynou z užívání nelegálního software, nese plnou odpovědnost uživatel, který porušení autorského zákona způsobil nebo jej připustil.

ČÁST XI.

PRAVIDLA ANTIVIROVÉ OCHRANY

Článek 49

Antivirová ochrana v síti

49.1 Instalaci a aktualizaci antivirového programu na všech běžných počítačích a virtuálních počítačích zajišťuje správce ICT.

49.2 Antivirový program se automaticky stará o antivirovou kontrolu v reálném čase (bez nutnosti zásahu uživatele) a plánované skenování na případný výskyt škodlivého kódu. Uživatel nesmí jakkoliv zasahovat do konfigurace antivirového programu, vypínat jej nebo jinak bránit jeho činnosti.

49.3 V případě výskytu škodlivého kódu nebo podezření na něj musí uživatel okamžitě přestat používat zařízení a tuto událost nahlásit jako bezpečnostní událost dle odst. 56.1.

Článek 50

Antivirová ochrana mobilních zařízení

50.1 Instalaci antivirového programu na noteboocích zajišťuje správce ICT. Uživatel je povinen zajistit aktualizaci antivirového programu a aplikaci bezpečnostních záplat na notebooku jeho připojením do datové sítě organizace nebo do internetu alespoň 1x za měsíc.

50.2 Za antivirovou ochranu ostatních mobilních zařízení (smartphone, tablet apod.), její instalaci a aktualizaci, odpovídá uživatel, jemuž bylo zařízení svěřeno do užívání.

ČÁST XII.

PRAVIDLA PRO OPUŠTĚNÍ PRACOVIŠTĚ

Článek 51

Neobsluhovaná zařízení

51.1 Trvale neobsluhovaná uživatelská zařízení

51.1.1 Trvale neobsluhovaným uživatelským zařízením se rozumí ta ICT zařízení, která jsou umístěna v technologických místnostech nebo zasedacích místnostech a tato zařízení nejsou trvale používána jedním uživatelem.

51.1.2 Uživatelé odpovídají za to, že neumožní přístup neoprávněným osobám k těmto zařízením, zejména, že řádně zabezpečí místnost při jejím opuštění a zamezí použití neobsluhovaného uživatelského zařízení jinou osobou např. odhlášením uživatelského účtu apod. Uživatelé také odpovídají za to, že na lokálních úložištích těchto zařízení nebudou ukládány žádné informace klasifikované vyšším stupněm než "VEŘEJNÉ".

51.1.3 V případě, že trvale neobsluhovaným zařízením je sdílené tiskové zařízení a hrozí, že na toto zařízení budou odeslány tisky jinými uživateli, nesmí uživatel ponechat v místnosti neoprávněnou osobu bez dozoru.

51.2 Dočasně neobsluhovaná uživatelská zařízení

51.2.1 Dočasně neobsluhovaným uživatelským zařízením se rozumí ta ICT zařízení, která jsou umístěna v kancelářích, kabinetech nebo třídách a na kterých uživatel dočasně přerušil nebo ukončil práci.

51.2.2 Uživatelé odpovídají za to, že při přerušení práce nebo ukončení práce na těchto zařízeních bude zajištěna jejich ochrana a ochrana v nich uložených informací. Zejména, že při opuštění počítače je zajištěno, že nebude možné zneužití uživatelského účtu jinou osobou (např. odhlášením, zamknutím plochy, apod.).

Článek 52

Zásada prázdného stolu a prázdné obrazovky monitoru

52.1 Uživatelé odpovídají za to, že při jakémkoliv opuštění kanceláře bude zachována ochrana informací v souladu se stupněm jejich klasifikace. Zejména, že v kanceláři nebudou volně dostupné informace klasifikované vyšším stupněm než "VEŘEJNÉ" a to v jakékoliv podobě analogové či digitální.

52.2 Uživatel je povinen zabezpečit pracoviště před jeho opuštěním. V případě, že na pracovišti nezůstává jiný zaměstnanec, je povinen pracoviště (kancelář apod.) řádně uzamknout.

52.3 Uživatel je povinen v případě krátkodobého opuštění pracoviště uzamknout počítač, aby chránil svůj uživatelský účet před neoprávněným použitím jinými zaměstnanci nebo cizími osobami.

52.4 Uživatel je povinen v případě opuštění pracoviště na delší dobu (více než 30 minut) ukončit všechny spuštěné aplikace a uzamknout počítač nebo se odhlásit z uživatelského účtu.

ČÁST XIII.

PRAVIDLA HLÁŠENÍ A ODSTRAŇOVÁNÍ PORUCH

Článek 53

Hlášení poruch a závad

53.1 Poruchy, závady a nefunkčnost informačních systémů a ICT zařízení patří mezi provozní události, se kterými se musí uživatel počítat.

53.2 Uživatel je povinen hlásit poruchy a závady příslušným správcům. Poruchy se oznamují přednostně prostřednictvím Helpdesku, příp. e-mailem nebo telefonicky.

53.3 Uživatel je povinen účinně spolupracovat se Správcem ICT a při odstraňování poruch a závad a dodržovat jejich pokyny. Pokyny nesmí být v rozporu s bezpečnostní politikou.

Článek 54

Poskytování uživatelské podpory a vzdálená pomoc

54.1 Uživatelskou podporu jsou oprávněni poskytovat pouze správci ICT, lokální správci a jimi pověřené osoby vybavené identifikační kartou "SERVIS ICT". Jiným osobám nesmí uživatel umožnit přístup k ICT prostředkům.

54.2 Uživatelská podpora může být poskytována osobně, telefonicky, e-mailem nebo systémem vzdálené pomoci, kdy může správce vzdáleně sledovat a ovládat počítač uživatele. O způsobu poskytnutí uživatelské podpory rozhoduje správce ICT nebo lokální správce.

54.3 Uživatelská podpora pomocí systému vzdálené pomoci smí být uživateli poskytována výhradně správcem ICT nebo lokálním správcem. Jiným osobám nesmí uživatel vzdálenou pomoc povolit.

54.4 Jediným schváleným systémem pro poskytování vzdálené pomoci je program TeamViewer, který je umístěn v datové síti organizace. Klientská část programu je opatřena logem města a zahájení relace je chráněno přístupovým heslem, které smí znát pouze správce ICT.

54.5 Relace vzdálené pomoci se navazuje spuštěním klientské části programu TeamViewer, sdělením devítimístného klientského identifikátoru "ID" správci a zadáním hesla správcem.

54.6 Během relace vzdálené pomoci nesmí uživatel opustit pracoviště a musí sledovat veškerou činnost správce. Po skončení relace je uživatel povinen ukončit program pro poskytování vzdálené pomoci.

ČÁST XIV.

PRAVIDLA PRO HLÁŠENÍ BEZPEČNOSTNÍCH UDÁLOSTÍ, INCIDENTŮ A SLABIN

Článek 55

Definice pojmů

55.1 Bezpečnostní událostí je každá událost, která může ohrozit bezpečnost informací (kterýkoliv z atributů: důvěrnost, dostupnost, integrita) nebo bezpečnost ICT prostředků v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky. Za bezpečnostní událost se považují také tyto události ve stadiu pokusu nebo vážného podezření.

55.2 Bezpečnostním incidentem je narušení bezpečnosti informací nebo narušení bezpečnosti služeb nebo bezpečnosti ICT prostředků v důsledku bezpečnostní události.

55.3 Bezpečnostní slabinou je zjištěný stav ICT prostředků nebo prostředí, který může způsobit vznik bezpečnostního incidentu.

55.4 Všechny tyto události musí být evidovány, analyzovány a musí být přijata opatření vedoucí k nápravě a návratu do bezpečného stavu.

Článek 56

Hlášení bezpečnostních událostí, incidentů a slabin

56.1 Všichni uživatelé jsou povinni neprodleně oznámit jakoukoliv bezpečnostní událost, incident a slabinu nebo podezření na ně lokálnímu správci, správci ICT, pověřenci nebo bezpečnostnímu správci. Hlášení bezpečnostních událostí, incidentů a slabin je možné písemně do helpdesku, 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.

56.2 Uživatel je povinen účinně spolupracovat s lokálním administrátorem, správcem ICT, pověřencem a bezpečnostním správcem při řešení bezpečnostních událostí, incidentů a slabin, zejména poskytovat jim úplné a pravdivé informace a dodržovat jejich pokyny. Pokyny nesmí být v rozporu s bezpečnostní politikou.

56.3 S výjimkou ustanovení odst. 56.1 a 56.2 uživatelé nesmí sdělovat informace o bezpečnostních událostech, incidentech a slabinách žádným dalším osobám.

Článek 57

Základní přehled bezpečnostních událostí a incidentů

57.1 Základní přehled bezpečnostních událostí, při nichž nedošlo k narušení bezpečnosti informací:

a) výpadek napájení,

b) přírodní nebo technická katastrofa, požár, výbuch, zátopy, prosakování tekutin, narušení konstrukce budov,

c) ztráta čipové karty nebo jiného prostředku pro autentizaci uživatele,

d) vyzrazení přístupového hesla,

e) výskyt škodlivého kódu,

f) poškození jakéhokoliv ICT prostředku,

g) porušení bezpečnostních opatření.

57.2 Základní přehled bezpečnostních incidentů, při nichž došlo k narušení alespoň jednoho atributu bezpečnosti informací:

a) výpadek napájení,

b) přírodní nebo technická katastrofa, požár, výbuch, zátopy, prosakování tekutin, narušení konstrukce budov,

c) neoprávněné nakládání s informacemi (vč. pořizování kopií papírových i elektronických dokumentů),

d) úmyslný nebo neúmyslný přístup neoprávněné osoby k ICT prostředkům nebo informacím,

e) poškození nebo zničení ICT prostředku, který je nositelem informací,

f) krádež nebo ztráta ICT prostředku, který je nositelem informací,

g) zneužití uživatelského účtu,

h) zneužití čipové karty pro přístup do budovy nebo k informačnímu systému,

i) připojení nepovoleného zařízení do datové sítě,

j) porušení bezpečnostních opatření.

ČÁST XV.

SOULAD S POŽADAVKY

Článek 58

Soulad s právními normami

58.1 Vytváření, zpracovávání a uchovávání informací a provoz veškerých souvisejících ICT prostředků musí být v souladu s právními normami závaznými v České republice a také smluvními podmínkami uvedenými v dohodách s dodavateli

zařízení a služeb.

58.2 Identifikace odpovídajících předpisů

58.2.1 Výchozí legislativou pro ochranu informací a provoz souvisejících ICT prostředků jsou:

a) zákon č. 365/2000 Sb., o informačních systémech veřejné správy

b) zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících předpisů

c) zákon č. 101/2000 Sb., o ochraně osobních údajů

d) zákon č. 227/2000 Sb., o elektronickém podpisu

e) zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

f) zákon č. 111/2009 Sb., o základních registrech

g) zákon č. 106/1999 Sb., o svobodném přístupu k informacím

h) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Nařízení eIDAS)

i) Směrnice Evropského parlamentu a Rady (EU) č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

58.2.2 Mimo těchto zákonů musí být v evidenci informačních aktiv uveden aktuální přehled všech právních norem, která vymezují způsob nakládání s informacemi nebo stanovují požadavky na provoz aktiva. Za aktuálnost a úplnost těchto informací odpovídá garant aktiva.

Článek 59

Uzavírání smluv

59.1 Pro zajištění odpovídající úrovně právní jistoty při uzavírání smluv souvisejících s provozem ICT prostředků musí být každá smlouva před uzavřením konzultována s právníkem. Ke každé takové smlouvě musí být konzultujícím právníkem vydána průvodka, ve které je uvedeno, zda navrhovaná smlouva obsahuje právní vady nebo jiná rizika a zda doporučuje uzavření smlouvy.

59.2 Za realizaci ochranných opatření dle odst. 59.1 odpovídá ředitel organizace nebo tajemník MMK.

Článek 60

Ochrana duševního vlastnictví

60.1 Všichni uživatelé jsou povinni dodržovat zákony na ochranu duševního vlastnictví, zejména pak zákon č. 121/2000 Sb., autorský zákon. Předmětem ochrany dle tohoto zákona jsou především programové vybavení a dokumenty, které jsou poskytovány jako licenční. Uživatelé nesou plnou odpovědnost za porušení povinností stanovených tímto zákonem.

60.2 Na všech ICT prostředcích organizace smí být instalováno a používáno pouze řádně licencované programové vybavení. Ke každému programovému vybavení musí existovat doklad o získání licence (faktura, licenční smlouva, licenční karta apod.). Je zakázáno instalovat programové vybavení, které není řádně licencováno.

60.3 V případě, že se programové vybavení poskytuje v rámci otevřené licence (např. freeware, open source software apod.), je nutné ověřit, zda se bezplatné užívání vztahuje také na užití soukromými a veřejnoprávními subjekty.

60.4 Musí být vedena evidence licencovaného software s počty licencí a evidence skutečně instalovaného programového vybavení.

60.5 Uživatelům musí být technickými prostředky znemožněna instalace vlastního programového vybavení na ICT prostředcích ve vlastnictví organizace nebo musí být zajištěna detekce takovýchto instalací.

60.6 Za realizaci ochranných opatření dle odst. 60.2 až 60.5 jejich správnou funkci odpovídá správce ICT a lokální správce.

Článek 61

Ochrana soukromí a osobních údajů

61.1 Všichni uživatelé jsou povinni dodržovat zákony na ochranu soukromí a osobních údajů, zejména pak zákon č. 23/1991 Sb., listina základních práv a svobod a GDPR. Předmětem ochrany jsou především listovní tajemství a tajemství jiných písemností a záznamů a osobní údaje. Uživatelé nesou plnou odpovědnost za porušení povinností stanovených těmito zákony.

61.2 Veškeré informační systémy, které slouží ke zpracování osobních údajů, musí být konfigurovány tak, aby je nebylo možné použít bez řádné autentizace a autorizace uživatele. Přístup uživatelů k těmto prostředkům musí být nastaven v

souladu se schváleným rozsahem přístupových práv. Za to odpovídá správce ICT a lokální správce.

61.3 Tato bezpečnostní politika obsahuje technická a organizační opatření správce osobních údajů dle čl. 32 GDPR.

ČÁST XVI.

ZÁVĚREČNÁ USTANOVENÍ

Článek 62

Porušení povinností vyplývajících z bezpečnostní politiky

62.1 Porušení povinností vyplývajících z Bezpečnostní politiky informací statutárního města Karviné bude zaměstnavatel posuzovat jako porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci.

62.2 Na základě individuálního posouzení závažnosti, míry zavinění a konkrétního rizika, případně míry dopadu a následků bezpečnostního incidentu způsobeného porušením výše uvedených bezpečnostních předpisů zaměstnancem, uskuteční potřebná opatření v souladu se zákoníkem práce případně předpisy souvisejícími, a to až po jednostranné rozvázání pracovního poměru. Porušení způsobená jinou osobou než zaměstnancem se budou posuzovat dle občanskoprávních předpisů. Tím není dotčena případná trestně právní odpovědnost.

Článek 63

Verze a schvalovací doložka

63.1 Tato Celková bezpečnostní politika informací (verze 4) ruší Celkovou bezpečnostní politiku (verze 3) schválenou Radou města Karviné dne 21.06.2017.

63.2 Tato Celková bezpečnostní politika informací (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

---

1) NSESSS = Národní standard pro elektronické systémy spisové služby.

2) např. § 303 zákona č. 262/2006 Sb., zákoník práce

3) např. Pracovní řád; Celková bezpečnostní politika informací

4) např. § 16 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů;

5) Např. zákon č. 499/2004 Sb., o archivnictví a spisové službě.