INTERNÍ SMĚRNICE VELITELE MĚSTSKÉ POLICIE BŘECLAV č. 1/2018

Správa a užívání informačních technologií

I. Úvodní ustanovení

1. Tato směrnice je vydána za účelem zajištění bezpečnosti a zvýšení stability informačních technologií (dále jen IT) Městské police Břeclav (dále jen MP), ochrany údajů v IT MP, snížení nákladů na provoz a opravy IT MP.
2. Pro práci v informačním systému (dále jen IS) MP platí zejména:
   - zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších změn a doplňků,
   - Nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
   - Standardy státního informačního systému (Úřad pro státní informační systém),
   - zákon č. 121/2000 Sb., autorský zákon, ve znění pozdějších změn a doplňků (dále jen autorský zákon),

II. Vymezení pojmů

1. Pojmem IT (informační technologie) nebo IS (informační systém) se pro účely této směrnice rozumí veškeré hardwarové (dále jen HW), softwarové (dále jen SW) a další technické prostředky a zařízení výpočetní techniky používané v prostorách MP nebo připojené do počítačové sítě MěÚ Břeclav.
2. Počítačová síť zahrnuje veškeré počítače a servery používané na MP a připojené k počítačové síti, SW instalovaný na těchto počítačích a serverech a veškeré technické zařízení zajišťující provoz počítačové sítě.
3. Počítač je osobní počítač (PC), notebook či obdobné zařízení (např. PDA, tablet,..) využívané pro běžnou práci uživatelů. Směrnice se vztahuje i na počítače nepřipojené k počítačové síti, pokud jsou v majetku MP.
4. Server je počítač vyhrazený pro poskytování síťových služeb ostatním počítačům a uživatelům počítačové sítě.
5. Technické zařízení zajišťující provoz počítačové sítě jsou zařízení a prostředky umožňující propojit počítače a servery do počítačové sítě a k Internetu (aktivní prvky, kabelové rozvody, zásuvky atd.).
6. Uživatel je každá osoba, zejména zaměstnanec MP, která používá některý z prostředků IT.
7. Správce prostředku IT je osoba pověřená správou některého z prostředků IT MP.
8. Legální SW je dílo (ve smyslu zejména odst. 2 § 2 autorského zákona), které má Město Břeclav, Městská policie Břeclav právo užít v rozsahu stanoveném licenční smlouvou uzavřenou s jeho autorem (dle § 46 autorského zákona) nebo nabyvatelem oprávnění (dle § 48 autorského zákona) nebo se jedná o dílo zaměstnanecké (dle § 58 autorského zákona), které autor/autoři vytvořil(i) ke splnění svých povinností vyplývajících

z pracovněprávního vztahu k Městské policii Břeclav, jakož i díla, která byla vytvořena na objednávku MP (dle odst. 7 § 58 autorského zákona).

III. Pravomoci a odpovědnost správců

1. Každý prostředek IT MP Břeclav musí mít stanoveného správce prostředku. Kde správce prostředku není určen, je správcem prostředku technik IT MP.
2. Technik IT MP je zodpovědný za IT MP jako celek. Podílí se na realizaci rozvoje IT v souladu se záměry MP a ve spolupráci s vedením MP.
3. Vedoucí oddělení informatiky a vnitřní správy MÚ je odpovědný za bezproblémový provoz celé počítačové sítě MP. Koordinuje tým podřízených zaměstnanců.
4. Správce HW je osoba pověřená údržbou HW na počítačích, serverech a technických zařízeních počítačové sítě.
5. Správce SW je osoba pověřená instalací údržbou SW vybavení na počítačích, serverech a konfigurací počítačů, včetně připojování a konfigurací tiskáren a podobně.
6. Správce uživatelů je osoba pověřená vedením evidence uživatelů (ve spolupráci s ostatními správci), přidělováním uživatelských jmen a hesel a správou přístupových systémů.
7. Správce prostředku IT odpovídá za technický stav prostředku a legálnost instalovaného SW. Správce prostředku IT je povinen upozornit na nelegálně instalovaný SW a požadovat jeho odstranění.
8. Pravomoci a odpovědnost správců jsou dány Organizačním řádem MP a definovány hierarchickým uspořádáním: ostatní správci jsou podřízeni správci počítačové sítě MÚ.
9. Uživatelé počítačové sítě jsou povinni respektovat pokyny vydávané příslušnými správci, pokud jsou v souladu s touto směrnicí nebo jsou objektivně odůvodnitelné vzhledem k okamžitému stavu IT s ohledem na zajištění bezproblémového provozu IT.

IV. Pravidla používání počítačové sítě MP a prostředků IT MP

1. Veškeré vybavení IT MP (HW a SW) je majetkem MP a je určeno pro plnění pracovních povinností zaměstnanců MP.
2. Každý zaměstnanec MP, který je uživatelem počítačové sítě MP, je povinen seznámit se s aktuálním zněním této směrnice a dodržovat ji, což potvrdí svým podpisem.
3. Uživatel nesmí vyvíjet takovou činnost, která by poškozovala IT MP nebo která by ostatním uživatelům škodila nebo bránila v řádném užívání IT MP.
4. Zaměstnanec MP je povinen řádně hospodařit se svěřeným IT vybavením a chránit ho před poškozením a zničením.
5. Porušení jakéhokoliv bodu této směrnice se považuje zejména za porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci dle zákoníku práce – viz článek 16. Závěrečná ustanovení směrnice.

V. Pravidla používání osobních počítačů/notebooků

1. Za dodržování pravidel při práci na osobním počítači či notebooku zodpovídá uživatel, kterému je počítač přidělen. Pokud je počítač/notebook přidělen více uživatelům, ten, který jej právě využívá.
2. Uživatel nesmí bez souhlasu správce HW zasahovat do HW konfigurace počítače. Případné problémy s HW řeší uživatel s příslušným správcem HW nebo prostřednictvím svého nadřízeného. Instalace SW provádí pouze správce SW, uživatel nesmí instalovat jakýkoliv SW ani nainstalovaný SW nijak modifikovat. Používání jiného než legálního SW MP je přísně zakázáno.
3. Uživatel je povinen vypnout nebo se odhlásit, popř. uzamknout pracovní stanici pomocí stisku kláves WIN+L nebo CTRL+ALT+DELETE, pokud opouští pracoviště.
4. Zaměstnanec nesmí přenosný počítač (notebook, tablet, PDA,..), který mu byl svěřen, v žádném případě svěřit jiné nebo cizí osobě a nesmí jej připojovat do cizích počítačových sítí. Dále ho nesmí používat k jiným účelům, než ke kterým mu byl svěřen. Pokud má zaměstnanec zřízen přístup k počítačové síti MP Břeclav prostřednictvím VPN připojení, nakládá s hesly a klíči, které mu byly předány, stejně jako ostatními hesly (viz 7.3).

VI. Tiskárny

1. Doplňování papíru zajišťuje uživatel tiskárny.
2. Výměnu toneru zajišťuje správce HW nebo jím pověřená osoba.

VII. Uživatelské účty, hesla, kódy, přístupový systém

1. Uživatelské účty v počítačové síti zřizuje a ruší správce uživatelů ve spolupráci se správci IT MP.
2. Správce uživatelů sděluje uživatelům přístupové informace vhodnou formou (nejlépe ústně), aby nemohlo dojít k jejich zneužití.
3. Uživatelé jsou povinni zachovávat mlčenlivost o svých přístupových informacích, aby nemohlo dojít k jejich zneužití. Za zneužití svých přístupových informací odpovídá uživatel, nebo ten, kdo uživateli tuto přístupovou informaci poskytl.
4. Uživatelé jsou povinni hesla měnit ve lhůtách nastavených v IS. Přitom dbají na to, aby se hesla do jednotlivých systémů od sebe vzájemně lišila. Pokud není určeno správcem jinak, musí se heslo skládat nejméně z osmi znaků a obsahovat nejméně jedno velké a malé písmeno a nejméně jeden znak nebo číslici.
5. Správce uživatelů je odpovědný za včasné zřizování, aktualizaci a zrušení přístupových práv a hesel pro uživatele prostředků IT MP. Personální oddělení MP s dostatečným předstihem a řádně informuje správce uživatelů o příslušných personálních změnách.

VIII. Údržba prostředků IT, odstávky

1. Pokud údržba IT vyžaduje dlouhodobější odstávku síťové služby či serveru, jsou o tom uživatelé včas informování (elektronickou poštou aj.). Tyto činnosti by měly být přednostně prováděny v době malého vytížení služeb a serverů.

2. O každém zásahu do HW či SW správce včas vyrozumí uživatele formou zprávy přes elektronickou poštu MP. Správce je povinen minimalizovat dobu nepřístupnosti služby a dopad na uživatele tak, aby nebyl ohrožen chod MP.
3. Bezpečnost a spolehlivost provozu má přednost před komfortem uživatelů.

IX. Pořizování HW, SW, řešení problémů s HW a opravy

1. Pořizování nového HW a SW spadá do kompetence příslušných správců HW a SW.
2. Uživatelé předávají své požadavky správcům HW a SW, ti zajišťují výběr vhodné varianty nákupu a koordinaci požadavků více uživatelů.
3. Návrh je po schválení správcem IT a velitelem MP předán k vlastní realizaci nákupu.
4. Při problémech s funkčností HW či SW je třeba se obrátit na příslušného správce, bez jeho vědomí se nesmí uživatel sám pokoušet závadu odstraňovat. Správce rozhodne o dalším postupu – nákup nového HW či SW, zajištění potřebné opravy. V závislosti na prioritě a zájmu činnosti MP správce zajistí bezodkladně dostupnost služeb a prostředků uživateli tak, aby nebyl ohrožen chod MP.

X. Připojování zařízení do počítačové sítě MÚ

1. Do počítačové sítě **MÚ** lze připojovat pouze počítače a obdobná zařízení, která jsou v majetku MP. Uživatel v žádném případě nesmí do počítačové sítě **MÚ** připojovat zařízení, které není v souladu s pravidly užívání IT prostředků MP (vlastní přenosné počítače, přenosné disky atd.) Jakékoliv přidělené přenosné zařízení smí uživatel používat pouze a jen v IT prostředcích MP, v souladu s plněním svých pracovních povinností.

XI. Datová úložiště

2. Pokud je k dispozici datové úložiště na některém ze serverů, je chráněno před přístupem ostatních uživatelů a jeho využití je plně v kompetenci uživatele.
3. Na serveru mohou být i sdílená datová úložiště přístupná definované skupině uživatelů a sloužící k výměně dat mezi těmito uživateli. Na tyto úložiště je zakázáno ukládat data obsahující osobní údaje, pokud není stanoveno jinak.
4. Pravidla chování uživatelů sdíleného datového úložiště a stupně oprávnění definuje správce a vhodnou formou je sděluje uživateli.

XII. Zálohování a archivace dat

1. Za data na osobním počítači zodpovídá uživatel.
2. Provozní data a nastavení serverů a síťové disky zálohují příslušní správci serverů nebo síťové služby.
3. Frekvence zálohování závisí na charakteru zálohovaných dat tak, aby nebyl ohrožen chod MP a případné ztráty byly co nejvíce minimalizovány.
4. Uživatelská data v datových úložištích mohou být zálohována, pokud to technické a kapacitní možnosti umožní. Důležitá data by si v každém případě měli uživatelé zálohovat sami. Pokud zálohovaná data obsahují osobní údaje, uživatelé odpovídají za bezpečnost těchto dat (např. kryptováním, uložením na nosič chráněný heslem apod.)

XIII. Informační systém MP Manager

1. Zaměstnanec MP vstupuje do systému pouze pod svým účet a heslem v souladu s výše uvedenými zásadami této směrnice.
2. Při vkládání osobních údajů do systému MP Manager odpovídá za to, že tato data odpovídají skutečnosti
3. Je zakázáno užívat pro zápis osobní data uložené ve starších záznamech bez řádného ztotožnění a kontroly se současným stavem.
4. Je zakázáno provádět lustrace, kategorizace, kopie, výpisy uložených údajů v systému mimo pracovní účely.

XIV. Elektronická pošta – Email

1. Každý zaměstnanec MP má vytvořeny dvě emailové adresy, na serveru MěÚ a na serveru MPBV.
2. Tyto emailové adresy jsou považovány za jedny z oficiálních kontaktů na daného uživatele.
3. Emailová adresy jsou zavedeny ve jmenném tvaru jmeno.prijmeni@breclav.eu a jmeno.prijmeni@mpbv.cz. Z důvodů organizačních jsou zavedeny tzv. hromadné adresy, např. _MP@breclav.eu, _vsmp@breclav.eu apd..
4. Emailová adresa je určena především ke komunikaci v pracovních záležitostech. V žádném případě nesmí být používána komerčně, např. k rozesílání obchodních sdělení daného uživatele apod.
5. Poštovní server je vybaven antispamovým a antivirovým SW. Tuto ochranu však nelze považovat za stoprocentní, a proto je třeba se chovat zodpovědně i na straně uživatele.
6. Vědomé rozesílání spamu z emailové adresy uživatele, z jeho počítače či serveru je zakázáno.

XV. Viry, antivirový SW

1. V rámci technických možností jsou na počítačích instalovány antivirové programy.
2. Uživatel nesmí antivirovou ochranu bezdůvodně vypínat nebo jinak oslabovat.

XVI. Řešení mimořádných událostí, chyb a požadavků

1. Pro řešení mimořádných událostí, chyb a požadavků je zřízena vzdálená pomoc dostupná přes aplikaci TeamViewer. Návod k použití této aplikace je dostupný na adrese http://wiki.meubv.local/doku.php?id=it:pomoc .
2. Každá událost nebo požadavek bude řešena přes IT technika MP. Událostí se myslí i požadavky na dodání drobného materiálu (tonery, myši apod.).
3. V případě závady HW, v jehož paměti jsou uložena data obsahující osobní údaje na toto uživatel upozorní IT technika, v případě jeho nepřítomnosti vedoucího pracovníka
4. Zaměstnanec MP neprodleně upozorní IT technika, v případě jeho nepřítomnosti vedoucího pracovníka i v případě podezření z neoprávněného přístupu do sítě, nebo IS nebo rizika takového neoprávněného přístupu, ztrátě nosiče obsahující nechráněná data obsahující osobní údaje (ztráta, vyzrazení hesla, ztráta paměťového zařízení apod.)

XVII. Likvidace datových nosičů, bezpečné mazání dat

1. Veškeré datové nosiče (diskety, CD-ROM, FLASH disky, pevné disky atd.) určené k vyřazení musí být odevzdány technikovi IT MP, který zajistí bezpečné smazání nebo likvidaci nosiče tak, aby minimalizovalo možnost obnovy dat z takového nosiče.

XVIII. Neobsluhovaná uživatelská zařízení

1. Musí být zajištěno zabezpečení neobsluhovaných zařízení a je po uživatelích vyžadováno, aby zajistili jeho přiměřenou ochranu dle následujících zásad:
   a) uzavřít aktivní relaci, jakmile je činnost ukončena. Tuto podmínku lze eliminovat v případě, kdy je zaveden vhodný mechanismus, např. spořič obrazovky s ochranou heslem s dobou spuštění pod 15 minut,
   b) odhlášení serverů a kancelářských PC, jakmile je končena relace (tj. nejenom pouze vypnout monitor, PC nebo terminál),
   c) zabezpečit PC nebo terminály před neautorizovaným použitím pomocí uzamčení klávesnice nebo jiným ekvivalentním opatřením, např. zajištění heslem, když není zařízení používáno.

XIX. Závěrečná ustanovení

1. Podle ustanovení § 180 Neoprávněné nakládání s osobními údaji zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších změn a doplňků, se posuzuje, kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, nebo poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.
2. Podle ustanovení § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. trestního zákoníku, ve znění pozdějších změn a doplňků, se posuzuje kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, nebo získá přístup k počítačovému systému nebo k nosiči informací a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,
3. Zaviněné porušení povinnosti vyplývající z této směrnice může být zaměstnavatelem posuzováno jako porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci ve smyslu zákoníku práce a Pracovního řádu MP. Zaměstnavatel při svém posouzení přihlédne ke konkrétním okolnostem, ke stupni intenzity, závažnosti či případnému opakování, zohlední i osobu zaměstnance a jeho

zavinění. Zaměstnavatel pak s ohledem na výše uvedené může porušení povinnosti se zaměstnancem projednat, snížit mu osobní příplatek nebo s ním ukončit pracovní poměr zaměstnance výpovědí ze strany zaměstnavatele ve smyslu § 52 odst. g) zákoníku práce.

4. Provedení nelegální instalace SW nebo vědomé využívání nelegálně nainstalovaného SW může být posuzováno jako závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci ve smyslu zákoníku práce a Pracovního řádu MP.
5. Pokud zaměstnanec nebude dodržovat tuto směrnici, vedoucí pracovník je oprávněn podat návrh na omezení nebo odebrání jeho práv k užívání prostředků IT MP.
6. Zaměstnanec odpovídá zaměstnavateli za škodu, kterou mu svým zaviněným jednáním způsobil. Zaměstnanec je povinen zaměstnavateli za podmínek stanovených zákoníkem práce způsobenou škodu nahradit.
7. Dnem účinnosti této směrnice se ruší Interní směrnici ředitele Městské policie Břeclav č. 6/2007 Správa a užívání informačních technologií včetně jejího Dodatku č. 1.
8. Tato směrnice nabývá účinnosti dnem. 13 -06- 2018

V Břeclavi dne 12.6.2018

Ing. Bc. Stanislav Hrdlička.
Velitel Městské policie Břeclav

MĚSTO BŘECLAV
MĚSTSKÁ POLICIE BŘECLAV
Kupkova 3, 690 02
tel.: 519 373 676