



Město Přestice

Rada města Přestice vydává tato

**Pravidla rady města Přestice č. 5/2018,
kterými se vydává provozní řád informačního systému města**

**Čl. 1
Předmět směrnice**

- (1) Touto směrnicí jsou stanovena vnitřní pravidla pro
- a) užívání výpočetní techniky (hardware) a programového vybavení (software),
 - b) užívání počítačové sítě města včetně všech počítačů a dalších technických zařízení (tiskárny, modemy, skenery, rozvaděče atd.), které jsou přímo nebo prostřednictvím jiného zařízení funkčně připojeny k počítačové síti města,
 - c) informační a datovou bezpečnost, včetně ochrany a zálohování elektronických dat a nakládání s hesly (heslová politika),
 - d) používání služeb internetu a elektronické pošty.
- (2) Ustanovení této směrnice jsou závazná pro všechny zaměstnance zařazené do orgánů a organizačních složek města i pro členy zastupitelstva města.

**Čl. 2
Základní pojmy, technické pojmy a zkratky**

- (1) Základní pojmy související s předmětem směrnice:
- a) **počítačová síť města** (dále jen „síť“) – všechna technická zařízení a programové vybavení používané při činnosti orgánů města, organizačních složek města, příspěvkových a městem zřizovaných organizací v budovách města k vzájemnému technickému a datovému propojení počítačů; síť spolu s přímo nebo nepřímo na síť připojenými počítači a jinými technickými zařízeními a programovým vybavením tvoří počítačový systém města (dále jen „systém“),
 - b) **počítač** (dále jen „PC“) – počítač ve vlastnictví města nebo oprávněně městem užívaný a připojený do sítě, případně fungující samostatně mimo síť,
 - c) **výpočetní technika města** (dále jen „výpočetní technika“) – všechny PC, ostatní zařízení informační techniky a všechny technické součásti sítě, které jsou ve vlastnictví nebo v oprávněném užívání města a jsou využívány při činnosti orgánů a organizačních složek města,

d) programové vybavení (dále jen „programy“) – programy a aplikace ve vlastnictví nebo v oprávněném užívání města, které jsou využívány při provozu výpočetní techniky,

e) uživatel – zaměstnanec, který je oprávněn užívat výpočetní techniku a programy,

f) uživatelské oprávnění – oprávnění uživatele ve vymezeném rozsahu užívat výpočetní techniku a programy; podmínky vzniku uživatelského oprávnění stanoví tato směrnice,

g) uživatelský účet – fyzické vyjádření uživatelského oprávnění; základními parametry jsou uživatelské jméno (login), heslo (password), definice přístupových práv a e-mailová adresa uživatele,

h) správce sítě – zaměstnanec zabezpečující podle této směrnice provoz výpočetní techniky, systému, sítě a plnící další úkoly stanovené touto směrnicí.

Čl. 3

Základní povinnosti a oprávnění

(1) Uživatel je oprávněn užívat výpočetní techniku, síť a programy v rozsahu svého uživatelského oprávnění a přístupových práv. Uživatel je povinen respektovat pokyny správce sítě, které vydá v souladu se svými oprávněními a povinnostmi.

(2) Uživatelem s uživatelským oprávněním je zaměstnanec, k výkonu jehož práce je nezbytné používání výpočetní techniky a programů.

(3) Výpočetní techniku a programy jsou oprávněni užívat pouze zaměstnanci s uživatelským účtem, a to v rozsahu svého uživatelského oprávnění a přístupových práv.

(4) Zaměstnancům je zakázáno:

a) poškozovat výpočetní techniku, programy nebo data nesprávným nebo neoprávněným užíváním,

b) používat výpočetní techniku, programy nebo data protiprávním způsobem nebo k protiprávní činnosti,

c) používat výpočetní techniku, programy nebo data k činnostem namířeným proti městu či proti jakémukoliv jinému subjektu, jehož počítačové prostředky jsou dostupné prostřednictvím sítě nebo prostřednictvím internetu,

d) umožnit přístup k výpočetní technice, programům nebo datům osobám, které nejsou oprávněnými uživateli podle této směrnice,

e) používat elektronické informace a data, k nimž nemají oprávněný přístup,

- f) používat elektronické informace a data, k nimž mají oprávněný přístup, způsobem, který je v rozporu s platnými právními předpisy nebo v rozporu s vnitřními předpisy města,
- g) kopírovat neoprávněně programy nebo jejich části,
- h) modifikovat neoprávněně programy a data,
- i) odposlouchávat neoprávněně provoz (komunikaci) v síti a vytvářet kopie elektronických informací či dat procházejících jednotlivými uzly sítě,
- j) instalovat jakékoliv programy, aplikace apod. bez výslovného souhlasu správce sítě,
- k) používat výpočetní techniku k soukromým účelům. Z tohoto pravidla je možné učinit pro konkrétní použití výjimku za předpokladu výslovného schválení nadřízeným zaměstnancem (tajemníka města) a zároveň správcem sítě. V tomto případě je však zaměstnanec povinen respektovat, že soukromé záležitosti lze v pracovní době a na pracovišti vyřizovat pouze výjimečně, v přiměřené a nezbytné míře a nesmí tím být dotčeno plnění povinností zaměstnance podle právních předpisů a podle vnitřních předpisů města.

Čl. 4

Používání výpočetní techniky

- (1) Uživatel je oprávněn užívat pouze výpočetní techniku, která mu byla řádně předána nebo jejíž užívání má zpřístupněno prostřednictvím výpočetní techniky, která mu byla řádně předána (např. sdílené tiskárny).
- (2) Výpočetní techniku je zaměstnanec oprávněn užívat pouze k činnostem souvisejícím s jeho prací a pouze v souladu se správným užíváním daného zařízení výpočetní techniky.
- (3) Pokud jde o technickou manipulaci s výpočetní technikou, je uživatel oprávněn pouze k běžným uživatelským činnostem, jako např. výměna toneru, cartridge, doplnění papíru v tiskárně, očištění monitoru, klávesnice, myši. Uživateli je zakázáno rozpojovat nebo přerušovat počítačovou síť, připojovat k síti nové PC nebo jakákoliv jiná technická zařízení, není-li dále uvedeno jinak. Manipulace s výpočetní technikou, které nesmí provádět uživatel, zabezpečuje správce sítě.
- (4) Závadu ve funkčnosti výpočetní techniky, je uživatel povinen neprodleně oznámit správci sítě. Veškeré opravy výpočetní techniky zabezpečuje pouze správce sítě.
- (5) Uživatel nesmí provádět změny konfigurace PC, jiných zařízení nebo zásahy do systému, které by mohly vést k jeho zhroucení, poruše nebo nežádoucímu chování. Jakékoliv nestandardní zásahy do konfigurace nebo systému je nutné předem projednat se správcem sítě.
- (6) Do sítě je zakázáno bez souhlasu správce sítě přímo nebo nepřímo připojovat jakákoliv technická zařízení, která uživatel nemá schválená k užívání.

(7) K PC je zakázáno připojovat přenosné a externí diskové jednotky včetně USB flash disků a CD/DVD nosičů, kromě zařízení schválených správcem sítě. V případě donesení dat v elektronickém formátu občanem na přenosném médiu je možné toto připojit do počítače až po zkontrolování správcem sítě.

Čl. 5

Používání programů

- (1) Uživatel je oprávněn užívat pouze programy, které mu byly řádně předány nebo jejichž užívání má zpřístupněno prostřednictvím výpočetní techniky, která mu byla řádně předána (např. programy a informační systémy serveru).
- (2) Programy je zaměstnanec oprávněn užívat pouze k činnostem souvisejícím s jeho prací a pouze v souladu s licenčními podmínkami a s příslušným návodem k danému programu.
- (3) Uživatelům je zakázáno stahování (downloading) dat nebo programů o velkém objemu (např. jde programové instalace, hudbu, video, filmy); zákaz se nevztahuje na automatické aktualizace nabízené systémem a oprávněně užívanými programy.
- (4) Bez předchozího souhlasu správce sítě je uživateli zakázáno instalovat jakékoliv programy.
- (5) Závadu ve funkčnosti programu je uživatel povinen neprodleně oznámit osobě pověřené za chod daného programu, případně správci sítě.
- (6) Město si vyhrazuje právo v odůvodněných případech v souladu s právními předpisy monitorovat spouštěné programy a dobu užívání jednotlivých programů zaměstnanci. Se zjištěnými údaji musí být nakládáno v souladu s ochranou soukromí a ochranou osobních údajů a s výsledky provedeného monitorování musí být zaměstnanec seznámen.

Čl. 6

Informační a datová bezpečnost

- (1) Každé PC je povinně vybaveno antivirovým programem a uživateli je zakázáno bez vědomí administrátora zasahovat do konfigurace antivirového programu. Je zakázáno aktivně vytvářet nebo šířit škodlivé programy a znemožňovat funkci ochranných programů.
- (2) Používání USB flash disků je umožněno pouze vybraným uživatelům při dodržení platných pravidel stanovených v článku 10.
- (3) Obdrží-li uživatel (na přenosném médiu, elektronickou poštou či jiným způsobem) jakýkoliv soubor z neznámé adresy, nebo o jehož původu lze důvodně pochybovat, je zakázáno soubor otevírat či ukládat na disk. Rovněž je zakázáno spouštět bez předchozí konzultace se správcem sítě spustitelné soubory došlé na přenosném médiu nebo elektronickou poštou, zejména pak soubory s koncovkami *.exe, *.com, *.bat., *.pif, *.vbs, *.vbe, *.msi.

(4) Má-li uživatel podezření na napadení PC virem, neprodleně informuje správce sítě a odpojí PC od sítě (výjimka z Čl. 4 odst. 3).

(5) Uživatel je oprávněn využívat pouze ta přístupová práva, která mu byla řádně přidělena. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla řádně přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci sítě a takto neoprávněně získaná přístupová práva nesmí využít. Uživatel dále nesmí zneužít chyby jiného uživatele (např. opomenuté odhlášení) k tomu, aby v síti pracoval pod cizí identitou nebo aby využil přístupová práva náležející jinému uživateli; na pracovištích s výpočetní technikou užívanou společně více uživateli je možné společné užívání přístupových práv, pokud byla takto nastavena.

(6) Elektronické informace a data přístupná prostřednictvím výpočetní techniky a sítě může uživatel využívat pouze, je-li k tomu oprávněn v rámci výkonu své práce a je-li to pro výkon jeho práce nezbytné. Uživatel je povinen při nakládání s daty dodržovat všechny související právní předpisy.

(7) Je zakázáno

a) zpřístupnit informace, které by mohly vést k narušení bezpečnosti a ochrany výpočetní techniky, sítě, programů nebo dat, umožnit jejich zpřístupnění neoprávněným osobám anebo tyto informace zveřejnit,

b) provádět jakékoliv činnosti, které vedou nebo mohou vést ke ztrátě nebo poškození dat,

c) získávat data patřící jiné osobě bez jejího výslovného souhlasu,

d) neoprávněně kopírovat nebo zálohovat data a tato data neoprávněně vynášet mimo objekty města nebo je neoprávněně předávat jiným subjektům,

e) použít nebo poskytnout jiným osobám neoprávněně získané klíče, dekodéry nebo jiné technické prostředky sloužící k zajištění informační a datové bezpečnosti a ochrany výpočetní techniky, sítě, programů nebo dat.

(8) Při opuštění pracoviště je uživatel povinen zabezpečit před zneužitím PC a data, která jsou jeho prostřednictvím přístupná (např. vypnutím, odhlášením nebo tzv. uzamčením PC).

(9) Město si vyhrazuje právo v odůvodněných případech v souladu s právními předpisy monitorovat dobu přístupu jednotlivých zaměstnanců na internetové stránky, včetně adres těchto stránek. V případě oprávněných a vážných důvodů může na příkaz tajemníka správce sítě po upozornění daného uživatele monitorovat jeho firemní e-mailovou komunikaci v rozsahu počtu došlých a odeslaných mailů včetně adres odesílatelů a příjemců, není však oprávněn je otevírat ani číst jejich obsah. Se zjištěnými údaji musí být nakládáno v souladu s ochranou soukromí a ochranou osobních údajů.

Čl. 8

Heslová politika

(1) Uživatelský účet a uživatelské oprávnění umožňuje jednoznačnou identifikaci uživatele při práci s výpočetní technikou a v síti. Součástí uživatelského účtu je i přidělení hesla opravňujícího ke vstupu do sítě. Mimo to vyžadují samostatné heslo i některé sdílené programy a společné datové složky a informační systémy. Prvotní hesla přiděluje správce sítě.

(2) Uživatel, který oprávněně zná a užívá dané heslo, odpovídá za to, že heslo nesdělí třetí osobě a bude uchováno na bezpečném místě. Následně je držitel hesla povinen heslo změnit vždy, je-li důvodná pochybnost, že heslo zná nebo může znát neoprávněná osoba.

(3) Pro tvorbu a používání hesel je nutné dodržovat následující zásady:

a) heslo musí uživatel uchovávat v tajnosti a chránit jej před zneužitím jinou osobou,

b) heslo musí být tvořeno tak, aby nebylo snadné jej odhalit, tedy heslo:

1. musí obsahovat alespoň jedno malé písmeno,
2. musí obsahovat alespoň jedno velké písmeno,
3. musí obsahovat alespoň jednu číslici (0–9),
4. musí obsahovat alespoň jeden speciální symbol z množiny znaků ! " # \$ % & ' () * + , - . : ; < = > ? @ [] ^ _ ` { | } ~
5. nesmí být tvořeno běžnými slovy a kombinacemi čísel přímo souvisejícími s držitelem hesla
6. minimální délka hesla musí být alespoň 8 znaků,
7. nedoporučuje se v heslech používat znaky s českou diakritikou,

c) nedoporučuje se zapisovat si heslo na papír nebo do datového souboru; pokud je heslo takto zapsáno, musí být záznam bezpečně uložen,

d) nedoporučuje se použití funkcí a programů pro zapamatování hesel, ani použití kombinace kláves PC pro vyvolání hesla.

Čl. 9

Používání internetu a elektronické pošty

(1) Každému uživateli je zpřístupněna prostřednictvím uživatelského PC internetová síť. Správce sítě může dle svého uvážení omezit přístup do Internetu zakázáním webových stránek, aplikací a protokolů, jež nejsou potřebné pro výkon pracovních povinností. V případě sporu rozhoduje o zakázání nebo povolení dané služby tajemník úřadu.

(2) Uživatel nesmí využívat přístup k webovým stránkám k soukromým účelům a zejména přístup k webovým stránkám s nebezpečným obsahem. Uživatel rovněž nesmí z pracovního PC nebo notebooku přistupovat ke své soukromé e-mailové schránce.

(3) Uživatel je oprávněn užít pracovní e-mailovou adresu pro osobní potřebu pouze v přiměřené a nezbytné míře.

(4) Je zakázáno odesílat z pracovní e-mailové adresy e-maily obsahující nevyžádaná data (spam) a data, která nemají pracovní charakter, nebo e-mailů s neslušným nebo nevhodným obsahem. Je zakázáno odesílání e-mailů s přílohami o velkém objemu dat, není-li to nutné pro splnění pracovního úkolu.

(5) Je zakázáno odesílat data a informace z počítačové sítě města na jiné e-mailové adresy než vyžaduje splnění pracovního úkolu, a to včetně vlastní soukromé e-mailové adresy uživatele.

Čl. 10

Používání USB úložných zařízení

(flashdisky, USB HDD, paměťové karty) – dále jen USB disk

(1) Uživatelé mohou používat USB disky jen se souhlasem správce sítě.

(2) Uživatel je povinen používat USB disk takovým způsobem, aby minimalizoval riziko jeho ztráty, odcizení nebo jiného zneužití.

(3) Na uživateli přidělený USB disk je zakázáno ukládat soukromá data.

(4) Uživatel je povinen pro zápis dat s osobními údaji používat pouze šifrovaný USB flash disk schválený správcem sítě.

(5) Uživateli je zakázáno z USB disku spouštět jakékoliv programy.

(6) USB disk smí být používán se zařízeními, jež nejsou v majetku města, pouze s výslovným souhlasem správce sítě. V takovém případě pak musí být USB disk vždy před dalším použitím v zařízení města zkontrolován správcem sítě.

(7) Při každém novém použití USB disku v zařízení města musí být tento zkontrolován uživatelem pomocí antivirového programu v daném zařízení. V případě jakéhokoliv pozitivního nálezu uživatel USB disk ihned vyjme, odpojí počítač od počítačové sítě (výjimka z Čl. 4 odst. 3), vypne dané zařízení a neprodleně informuje správce sítě.

(8) V případě ztráty USB disku je dotyčný povinen ztrátu okamžitě nahlásit správci sítě a svému nadřízenému

Čl. 11

Vypalování dat na CD nebo DVD média

(1) Vybraným uživatelům je povoleno vypalování dat na CD nebo DVD média a to na základě souhlasu nadřízeného pracovníka a správce sítě.

(2) Uživatel nesmí používat vypalování dat na CD nebo DVD média k soukromým účelům.

(3) Uživatel je povinen používat CD nebo DVD média s pracovním obsahem takovým způsobem, aby minimalizoval riziko jeho ztráty, odcizení nebo jiného zneužití.

(4) Uživatel je povinen používat pro vypalování dat pouze software schválený správcem sítě.

(5) V případě vypalování dat s osobními údaji je nutné použít šifrování dat a zabezpečení heslem.

Čl. 12

Ukládání a zálohování dat

(1) Pravidelně jsou zálohována data v informačních systémech města (Radnice VERA, VITA, MS Exchange, ...)

(2) Data uložená v PC jsou zálohována, případně i verzifikována po dohodě se správcem sítě. Standardně je možno zálohovat složku „Dokumenty“, po dohodě se správcem sítě je možné zálohovat i jinou složku.

(3) Pro ukládání dat je nutné dodržovat následující zásady:

- a) soubory v PC ukládá uživatel do složky Dokumenty
- b) jiné složky pro ukládání dat používá uživatel výhradně se schválením správce sítě
- c) s ohledem na velikost místa na disku je uživatel povinen smazat nepotřebné soubory a e-mailové zprávy.

(4) Případný lokální soubor .pst s rozšířením e-mailové schránky uživatele není automaticky zálohován.

(5) Data, která nebudou uložena podle stanovených zásad, nejsou zálohována.

(6) Pokud uživatel potřebuje zálohovat data některého programu, je povinen tuto skutečnost nahlásit správci sítě, který zajistí jejich zálohování.

(7) Případnou ztrátu nebo poškození dat je uživatel povinen okamžitě nahlásit správci sítě, který zajistí jejich případnou obnovu ze zálohy.

(8) Servery se zálohují každou noc, přičemž se uchovává minimálně posledních 30 záloh. Minimálně posledních 7 záloh je pak ukládáno duplicitně v budovách na Masarykově náměstí 107 i v Husově 465.

Čl. 13

Závěrečná ustanovení

(1) Obsahují-li pravidla rady města nebo vnitřní směrnice vydané před účinností těchto pravidel ustanovení odlišná, platí ustanovení těchto pravidel.

(2) Vydání této směrnice bylo schváleno usnesením RM č. 560 /2018 ze dne 8.10.2018 a současně ruší Pravidla rady města Přestice č. 3/2018, kterými se vydává provozní řád informačního systému města schválená pod usn. č. 291/2018 ze dne 14. 5. 2018.

(3) Tato směrnice nabývá účinnosti dnem 9.10.2018.

Karel Naxera

Mgr. Karel Naxera
starosta



Marek Krivda
Marek Krivda
místostarosta