

## Města Řevnice



---

# Řád provozování Informačního systému úřadu

# Obsah

<b>1. Úvodní ustanovení.....</b>	<b>3</b>
1.1. Definice základních pojmů.....	3
1.2. Správce Informačního systému úřadu .....	3
1.3. Provozovatel Informačního systému úřadu.....	4
1.4. Nakládání s informacemi.....	5
1.5. Odpovědnost organizačních a řídicích struktur.....	6
1.6. Odpovědnost výkonných struktur (z hlediska IS úřadu).....	8
<b>2. Provozní řád.....</b>	<b>11</b>
2.1. Obecné zásady práce s výpočetní technikou .....	11
2.2. Provozní doba sítí .....	13
2.3. Pohotovost pro uživatele .....	13
2.4. Semináře, školení .....	13
2.5. Archivace a zálohování datových souborů.....	14
2.6. Elektronická pošta.....	14
2.7. Antivirová bezpečnost .....	15
2.8. Internet.....	16
2.9. Přístup mobilních uživatelů k IS úřadu.....	16
2.10. Vytváření přístupů uživatelů k IS úřadu .....	16
2.11. Změna a rušení přístupů uživatelů k IS úřadu .....	17
2.12. Publikování informací .....	17
<b>3. Závěrečná ustanovení .....</b>	<b>18</b>
<b>4. Přílohy .....</b>	<b>18</b>

# 1. Úvodní ustanovení

Řád provozování Informačního systému Městského úřadu Řevnice (dále jen „úřad“) vymezuje obsah pojmu Informační systém úřadu. Je závazným předpisem pro všechny osoby v pracovním, nebo jiném obdobném poměru k úřadu, tj. všechny uživatele Informačního systému úřadu, včetně osob vykonávajících veřejné funkce v rámci správního území úřadu.

## 1.1. Definice základních pojmů

V dokumentu jsou používány některé pojmy, jejichž význam je vysvětlen v samostatném materiálu Výkladový slovník Informačního systému úřadu.

## 1.2. Správce Informačního systému úřadu

Správce Informačního systému úřadu (dále jen IS) je úřad.

Správce IS úřadu:

- zodpovídá za vývoj a provoz IS úřadu v souladu s platnými právními předpisy a závaznými dokumenty, zejména:
  - zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění zákona č. 517/2002 Sb., v platném znění,
  - zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, v platném znění,
  - zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, v platném znění,
  - zákon č. 148/1998 Sb., o ochraně utajovaných skutečností, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek, v platném znění,
  - zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek, v platném znění,
  - zákonem č.240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) především § 27, v platném znění,
  - nařízením vlády č.462/2000 Sb k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon),
  - nařízením vlády č. 495/2005 Sb., o elektronickém podpisu,
  - vyhláškou č. 496/2004 Sb., o elektronických podatelkách,

- vyhláškou č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup, v platném znění
  - zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů,
  - zákonem č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů,
  - vyhláškou č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti).
- stanovuje podmínky vývoje a provozu IS úřadu v rámci základních dokumentů typu Informační strategie, Informační koncepce, Bezpečnostní politika, ...
  - vytváří obecná pravidla pro zpracovávání, využívání a zveřejňování dat a informací.

### 1.3. Provozovatel Informačního systému úřadu

Provozovatelem IS úřadu je Kancelář tajemníka a informatik-správce sítě.

Na základě pokynů vedení úřadu zajišťuje:

- realizaci Strategie implementace eGovernmentu v území, Informační strategie kraje/regionu, Informační strategie úřadu, Bezpečnostní politiky IS úřadu, ...
- přípravu rozpočtu investičních a provozních nákladů IS úřadu v jednotlivých finančních rocích.

Na základě požadavků uživatelů zajišťuje zejména:

- plánování, nákup, instalaci a údržbu veškerého software a hardware včetně kabeláže počítačové sítě,
- plánování a nákup spotřebního materiálu,
- konzultace, školení a další služby související s podporou uživatelů.

Dále zajišťuje:

- nákup, přebírání datových souborů od externích organizací, jejich transformaci do IS úřadu a zprovoznění příslušné autonomní agendy, která tyto soubory zpracovává,
- poskytování datových souborů externím organizacím včetně jejich transformace z IS úřadu,

- koordinaci spolupráce se subjekty stojícími mimo úřad, které se podílejí na rozvoji a provozu IS úřadu,
- provoz lokálních počítačových sítí a jejich napojení na externí datové sítě,
- pravidelnou archivaci dat na serverech a poskytuje klientům prostředky pro archivaci dat na lokálních stanicích,
- udržování veškeré dokumentace k IS úřadu.

Provozovatel IS úřadu je povinen:

- provést hardwarovou a softwarovou konfiguraci pracoviště pro uživatele na základě kompetencí, kterými je uživatel vybaven. Tyto kompetence určí konkrétnímu uživateli garant úlohy, obvykle jeho bezprostřední přímý nadřízený,
- zajistit v maximálně možné míře ochranu před neoprávněnými přístupy k síťovým i lokálním prostředkům a před napadením počítačovými viry,
- stanovit režim pravidelné archivace dat,
- plánovat a provádět pravidelnou profylaxi hardware a ověřování funkčnosti software.

## 1.4. Nakládání s informacemi

Provozovatel i každý uživatel IS úřadu musejí respektovat následující zásady nakládání s informacemi:

- Informace vznikající činností úřadu na všech jeho pracovištích jsou součástí majetku úřadu.
- Informace, které úřad zakoupil, jsou majetkem úřadu a současně na ně mohou být vázány smluvní podmínky o způsobu nakládání s informacemi mezi organizací, která se na vzniku nebo zprostředkování informací podílí.
- Zpracovávání a uchovávání osobních údajů může být realizováno pouze v rámci zákona č. 101/2000 Sb., o ochraně osobních údajů. V podmínkách MěÚ Řevnice je provádění těchto činností ošetřeno interní Směrnicí pro práci s osobními údaji (č. 1/2010).

Uživatelé jsou povinni zejména:

- nezprostředkovat ani nezpřístupnit tyto údaje třetí osobě, právnické ani fyzické, pokud to přímo neukládá zákon,
- nevyužít tyto údaje pro jiný účel, než pro který jsou shromažďovány,
- umožnit občanovi na požádání nahlédnutí do záznamů, které jsou o něm vedeny.

Postih za neoprávněné nakládání s osobními údaji řeší zejména zákon č. 140/1961 Sb. - Trestní zákon, ve znění pozdějších předpisů, zvláště pak § 178 a dále zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

- Zprostředkování údajů z IS úřadu fyzické či právnické osobě je možné pouze tehdy, je-li to nezbytně nutné pro plnění úkolů uložených příslušným právním předpisem, a pokud to předpis připouští a to v rozsahu, který je tímto předpisem určen.
- Pokud se jedná o zprostředkování dat většího rozsahu v elektronické podobě nebo ve formě sestavy, je nutné jejich předání zaznamenat do předávacího protokolu. Vždy musí být vymezeny vzájemné odpovědnosti za bezpečnost dat. Formu a obecný obsah poskytovaných dat určuje správce IS úřadu. Správce IS úřadu navrhuje i cenu, za kterou jsou konkrétní data z IS úřadu poskytována. Vlastní realizaci poskytování dat zajistí provozovatel IS úřadu.
- Přebírat datové soubory z externích zdrojů do IS úřadu lze pouze na základě smluv, obchodních ujednání, provozních předpisů a v souladu s tímto řádem. Vždy musí být vymezeny vzájemné odpovědnosti za bezpečnost dat. Důvodem pro toto opatření je ochrana úřadu a jeho informačního systému před nekonzistentními daty.

Formu a obecný obsah poskytovaných dat určuje správce IS úřadu, který musí vyjádřit i souhlas s cenou, za kterou jsou konkrétní data do IS úřadu přebírána.

Přebírání dat zajišťuje informatik-správce sítě, který provede kontrolu převzatých datových nosičů (například z důvodu ochrany před počítačovými viry), kontrolu převzatých datových souborů a jejich zařazení do IS úřadu. Pracovník realizující převzetí dat je zodpovědný za jejich ochranu před zneužitím neoprávněnými osobami.

## 1.5. Odpovědnost organizačních a řídicích struktur

### 1.5.1. Orgány města

Orgány města (zastupitelstvo, rada, starosta) na základě svých pravomocí daných jinými předpisy zastávají ve vztahu k provozování IS úřadu následující funkce:

- Schvalují rozpočet na rozvoj a provoz IS úřadu pro běžný finanční rok.
- Jmenují členy komisí či pracovních skupin pro informační technologie.
- Stanoví zásady a cenové podmínky pro výdej příp. prodej dat externím subjektům.

### 1.5.2. Úřad – zastoupený tajemníkem

- Pověřuje odbory provozováním a správčovstvím subsystémů a úloh, jakož i garancí za jejich správnost a funkčnost.
- Schvaluje předpisy pro způsob přebírání a využívání dat z externích zdrojů (oprávnění k přístupu, další poskytování, ochrana, ...).

### 1.5.3. Kancelář tajemníka ve spolupráci s informatikem-správcem sítě

Zajišťuje mimo jiné i tyto činnosti:

- koncepční a projektové činnosti (příprava koncepce, příprava metodologií a postupů, příprava a řízení projektů),
- správu financí určených pro informační technologie (příprava rozpočtu, čerpání finančních prostředků),
- administrativní činnosti odboru (evidence písemností, tvorba předkladů, materiálů a dalších písemností, příprava a evidence smluv, evidence úkolů, komunikace s dodavateli),
- analytické a metodické činnosti (sběr a třídění uživatelských požadavků, analytické a metodické práce),
- programátorské činnosti (programování pro Internet a Intranet, tvorba webdesignu a grafické práce),
- informování a vzdělávání,
- pravidelnou archivaci dat,
- přípravné práce (získávání software, úprava pracoviště, instalace klientského pracoviště),
- administrátorské činnosti (administrace bezpečnostního systému, aplikačních informačních systémů, databázových, operačních, komunikačních a publikačních systémů),
- provozní a servisní činnosti (údržba uživatelských účtů, údržba domovských adresářů, uživatelská podpora a řešení problémů uživatelů, konfigurace aplikačního software, instalace a ověřování funkčnosti software, plánování a provádění pravidelné profylaxe hardware, údržba a opravy hardware, nákup a výdej spotřebního materiálu, operativní evidence techniky),
- zpracování podkladů pro Intranet a Internet,
- tisk grafických materiálů, propagačních materiálů dle potřeb úřadu (pozvánky, vizitky atd.).

#### **1.5.4. Vedoucí odborů**

Předávají informatikovi-správci sítě požadavky na rozvoj a dodávky hardware, software, školení, respektive služeb dle potřeb pro zajištění činnosti vlastního odboru v rámci pravidel definovaných v provozní dokumentaci (viz přílohy).

Odpovídají za kvalifikované využívání prostředků IS úřadu.

#### **1.5.5. Vedoucí oddělení**

Definují vedoucím odborů obecné požadavky na konfiguraci klientských pracovišť, zdrojů dat a přístupová práva jednotlivých klientů k prostředkům IS úřadu.

Pověřují konkrétní zaměstnance správou klientských pracovišť.

Odpovídají za dodržování provozních a bezpečnostních zásad.

Odpovídají za efektivní využívání prostředků IS úřadu.

### **1.6. Odpovědnost výkonných struktur (z hlediska IS úřadu)**

#### **1.6.1. Garant úlohy**

Je zodpovědný za metodickou náplň úlohy, v rámci ověřovacího provozu potvrzuje správnost jejího řešení a podílí se na zpracování provozní dokumentace. Obvykle je garantem úlohy vedoucí oddělení, pro kterého byla úloha vytvořena.

#### **1.6.2. Správce úlohy**

Odpovídá za to, že úloha bude využívána dle provozní dokumentace.

V případě úloh určených pro jediného uživatele bude správcem úlohy obvykle tento uživatel. Pro úlohy určené pro jediné oddělení bude obvykle správcem úlohy pracovník pověřený vedoucím tohoto oddělení. Pro úlohy určené pro jediný odbor bude obvykle správcem úlohy pracovník pověřený vedoucím tohoto odboru. V případě úloh přístupných více než jednomu odboru určuje správce úlohy tajemník úřadu.

Správce úlohy je povinen sledovat stav programu, závady a neobvyklé projevy hlásit informatikovi-správci sítě provádět údržbu programu a dat v rámci svého oprávnění, sumarizovat poznatky uživatelů a předávat je informatikovi-správci sítě. Ustanovení správce pro určitou úlohu a rozsah jeho oprávnění navrhuje informatik-správce sítě, schvaluje vedoucí odboru. Tam, kde je to potřebné vzhledem k specifickým vlastnostem technického nebo programového vybavení pracoviště, může správce úlohy se souhlasem vedoucího odboru pověřit pracovníka odboru prováděním určité přesně dohodnuté činnosti, resp. oprávnit ho k jejímu provádění.



### 1.6.3. Správce datového souboru

Obvykle bývá správcem datového souboru ten, kdo provádí nejčastěji změny datových položek v tomto souboru.

Správce datového souboru odpovídá za:

- včasné pořízování, případně aktualizaci datového souboru dle provozní dokumentace,
- zajištění všech vazeb vůči ostatním souborům báze dat IS úřadu,
- archivaci datového souboru dle provozní dokumentace a v předepsaném termínu.

### 1.6.4. Správce koncového pracoviště

Obvykle bývá správcem koncového pracoviště určen jeho nejčastější uživatel. Správce koncového pracoviště je určen vedoucím odboru.

Odpovídá za předané pracoviště, dodržování obecných zásad práce s výpočetní technikou a provozních a bezpečnostních podmínek, které se na pracoviště vztahují. Tyto podmínky jsou kromě tohoto řádu stanoveny i dalšími vnitřními směrnici úřadu (např. Pracovní řád, Pravidla bezpečnosti práce a ochrany zdraví, apod.).

K zajištění toho má k dispozici:

- protokol pracoviště,
- provozní dokumentaci k pracovišti dodanou dodavatelem.

Správce koncového pracoviště je povinen:

- převzít pracoviště a podepsat protokol. Dále je povinen podepisovat následné změny v konfiguraci pracoviště.
- sledovat stav všech zařízení náležících ke koncovému pracovišti a každou změnu, závadu nebo neobvyklý projev hlásit informatikovi-správci sítě, případně správci úlohy,
- zamezit neoprávněnému využití pracoviště.

Správce koncového pracoviště smí kontaktovat pracovníky externích dodavatelů (objednávání produktů a služeb, potvrzování dodacích či servisních listů, instalace software a hardware) pouze za přítomnosti tajemníka a informatika-správce sítě.

### 1.6.5. Uživatel koncového pracoviště

Uživatelem koncového pracoviště je osoba, která s tímto pracovištěm pracuje.

Uživatel smí používat pracoviště pouze v rámci své pracovní náplně. Pro práci v autonomním režimu je uživatel registrován správcem koncového pracoviště. Pro práci v síťovém režimu je registrován informatikem-správce sítě, který mu

také přidělí přihlašovací jméno. Uživatele koncového pracoviště a rozsah jeho oprávnění určuje vedoucí odboru.

Pracovníkovi je povolen samostatný přístup k IS úřadu až po školení, resp. zaškolení v rozsahu určeném informatikem-správcem sítě v závislosti na rozsahu uživatelského oprávnění.

Uživatel koncového pracoviště:

- je povinen dodržovat provozní podmínky stanovené či vyžadované provozovatelem (vhodné prostředí, antivirová ochrana, termíny zpracování úloh nebo aktualizace datových souborů), řídit se obecnými zásadami práce s výpočetní technikou, provozním řádem IS úřadu, pokyny provozovatele IS úřadu, příp. správce koncového pracoviště nebo správce úlohy,
- musí používat při práci s IS úřadu výhradně jméno a heslo dle podmínek stanovených provozovatelem IS úřadu.,
- musí respektovat přidělená přístupová práva k IS úřadu, nesmí se pokoušet o neoprávněné získání jiných přístupových práv,
- nesmí sdělovat své uživatelské jméno, heslo a přístupová hesla k IS úřadu třetím osobám kromě svého nejbližšího nadřízeného,
- nese odpovědnost za případné zneužití informací, které patří do kategorie chráněných (služební, osobní a citlivá data, strategické informace,...),
- je povinen dodržovat předepsané postupy při zpracování agend,
- je povinen nepřipustit změnu hardwarové a softwarové konfigurace pracoviště bez souhlasu provozovatele IS úřadu,
- je povinen nahlásit včas provozovateli IS úřadu veškeré funkční a bezpečnostní, případně organizační nedostatky,
- je povinen seznámit se způsobem zálohování dat, se kterými pracuje. V případě, že je uživateli přidělen režim jeho vlastního zálohování, je povinen tento režim dodržovat. Uživatel je rovněž povinen seznámit se se způsobem antivirové ochrany zavedeným na pracovišti a používat ho při své práci.

Uživatel koncového pracoviště smí kontaktovat pracovníky externích dodavatelů (objednávání produktů a služeb, potvrzování dodacích či servisních listů, instalace software a hardware) pouze za přítomnosti informatika-správce sítě.

#### **1.6.6. Servisní pracovník (informatik - správce sítě)**

Problémy, závady, případně požadavky související s provozem IS úřadu oznamují uživatelé servisním pracovníkům odboru informatiky podle pravidel definovaných v provozním řádu a jeho přílohách.

## 2. Provozní řád

### 2.1. Obecné zásady práce s výpočetní technikou

V IS úřadu smí být používáno pouze programové vybavení, pro které má úřadu platnou licenci, a pouze v rozsahu této licence. Nesmějí být používány žádné neoprávněné kopie libovolného programového vybavení. O oprávněnosti instalace a používání programového vybavení rozhoduje provozovatel IS úřadu.

Uživatel je povinen dodržovat následující zásady:

#### 2.1.1. Zásady umístění a zapojení PC a tiskáren

O umístění PC a tiskáren rozhoduje informatik-správce sítě tak, aby byla dodržena všechna nařízení a závažná doporučení výrobce zařízení a splněny požadavky na bezpečnost práce. Bez konzultace s informatikem-správcem sítě nelze zvolené umístění měnit.

Do stejné zásuvky s počítačem nebo tiskárnou je zakázáno zapojovat jiné spotřebiče (např. ponorný vařič, ventilátor, kopírka, infrazářič, rádio).

Provádění změn v propojení mezi zařízeními je vyhrazeno informatikovi-správcí sítě.

#### 2.1.2. Zásady péče o PC

Při čištění zařízení a příslušenství používat čisticích prostředků doporučených informatikem-správcem sítě. Zařízení čistit při vypnutém napájení a způsobem schváleným informatikem-správcem sítě..

Nepohybovat PC, pokud je zapnutý.

Nevypínat PC při krátkodobém přerušení práce. PC znovu nezapínat bezprostředně po vypnutí (minimální prodleva 1 minuta). Při výpadku napájení PC nebo terminál vypnout.

Neotevírat kryty zařízení.

V blízkosti PC nekouřit.

Jakékoliv závady oznámit provozovateli IS úřadu (případně prostřednictvím správce koncového pracoviště nebo úlohy).

#### 2.1.3. Zásady péče o tiskárnu

Dodržovat pracovní postupy stanovené provozovatelem IS úřadu pro jednotlivé typy tiskáren na základě nařízení a doporučení výrobce.

Nepoužívat poškozená nebo nekvalitní média, např. papíry, obálky a samolepicí štítky.

Věnovat pozornost kontrole a přípravě papíru při zakládání do podavačů (ohnutí, prolisování, síla svazku).

Věnovat pozornost směru přiváděného i odváděného perforovaného papíru a jeho skládání.

Síťovou tiskárnu připojenou k terminálu zapínat vždy až po zapnutí terminálu.

Jakékoliv závady oznámit informatikovi-správci sítě (případně prostřednictvím správce koncového pracoviště nebo správce úlohy).

#### **2.1.4. Zásady péče USB disky a paměťová média**

Paměťová média uchovávat v obalu (pouzdro, box, krabička).

Smějí být používány pouze USB disky a paměťová média zakoupené a poskytnuté prostřednictvím odboru informačních technologií. Jakékoliv jiné USB disky a paměťová média, které byly použity za účelem přenesení dat z jiné sítě, musí být nejprve předloženy pracovníkovi odboru informačních technologií na překontrolování.

Zavirování sítě IS úřadu způsobené nesprávným použitím USB disků a paměťových médií se považuje za hrubé porušení provozního řádu IS.

Jakékoliv závady/poruchy spojené se špatným čtením USB disků a paměťových médií popř. jejich nefunkčností oznámit informatikovi-správci sítě.

#### **2.1.5. Zásady ochrany dat**

Dodržovat předepsaný režim zálohování a archivace dat.

Při podezření na ztrátu nebo poškození dat přerušit práci a informovat informatika-správce sítě.

Poškozené paměťová média a média nejasného obsahu vracet informatikovi-správci sítě.

Ochraňovat data na paměťových médiích před neoprávněnou manipulací a ztrátou. V případě ztráty hlásit tuto skutečnost informatikovi-správci sítě. i s popisem ztracených či zcizených dat, které mohou být zneužity jinou osobou.

Před vypnutím počítače a před opuštěním pracoviště (i krátkodobým) uzavřít aplikační programy i textové a tabulkové soubory. Neponechávat programy a soubory zbytečně otevřené po dokončení práce.

#### **2.1.6. Další povinnosti uživatele**

Používat aplikační vybavení pouze v rozsahu daném jeho pracovní náplní a v souladu s uživatelskými příručkami.

Dodržovat režim zálohování dat, byl-li mu přidělen.

Respektovat přidělená přístupová práva k IS úřadu, nepokoušet se o neoprávněné získání jiných přístupových práv

Neumožnit přístup a využívání přiděleného PC neoprávněným uživatelům.

Neinstalovat samostatně jakékoliv programové vybavení

## 2.2. Provozní doba sítí

Základní doba provozu sítí je shodná s pracovní dobou stanovenou platným Pracovním řádem:

pondělí	od 7.30	do 18.00 hodin
úterý	od 7.30	do 15.00 hodin
středa	od 7.30	do 18.00 hodin
čtvrtek	od 7.30	do 15.00 hodin
pátek	od 7.30	do 13.00 hodin

V případě potřeby je nutné předem požádat informatika-správce sítě o zajištění plné funkčnosti sítě mimo základní provozní dobu. Jedná se například o jednání zastupitelstva a rady, jednání výborů a komisí.

Mimo tuto dobu jsou prováděny administrativní úkony typu archivace, profylaxe, kontrolní chody atp. Během těchto činností může dojít k nižší průchodnosti sítě, případně k úplnému odstavení některých programů.

Zcela výjimečně (řešení havarijních stavů, nutná spoluúčast externích dodavatelů) může být provoz sítě omezen i v základní provozní době. O této situaci musí být předem všichni uživatelé (prostřednictvím vedoucích odborů) vyzooměni vedoucím oddělení provozního a servisního.

## 2.3. Pohotovost pro uživatele

Uživatelům jsou během výše uvedené základní provozní doby sítí k dispozici servisní pracovníci – informatik sítě, kteří jsou pověřeni podporou uživatelů.

V případě poruchy či havárie nahlásí uživatel neprodleně tuto skutečnost informatikovi-správci sítě a při řešení problému poskytuje servisnímu pracovníkovi potřebnou součinnost.

## 2.4. Semináře, školení

Informatik-správce sítě vyhlašuje témata seminářů a školení prostřednictvím vedoucích odborů na poradě tajemníka úřadu a na Intranetu. Všichni zájemci o školení či seminář se musí přihlásit k účasti pověřenému pracovníkovi na odboru informatiky a to prostřednictvím elektronické pošty, telefonu či osobně.

Každý nový uživatel IS úřadu je povinen absolvovat všechny lekce školení dle Koncepce vzdělávání v oboru výpočetní techniky úřadu dostupné na Intranetu.

## 2.5. Archivace a zálohování datových souborů

Data na serverech archivuje provozovatel IS úřadu způsobem, v rozsahu a termínech stanovených provozní dokumentací.

Data na lokálních stanicích archivuje správce úlohy způsobem, v rozsahu a termínech stanovených provozní dokumentací.

Provozovatel IS nemůže zaručit obnovu dat a nenesе žádnou odpovědnost za ztrátu dat uložených na lokálních stanicích, USB discích a paměťových médiích.

## 2.6. Elektronická pošta

Elektronická pošta je určena pro služební účely. Využívání elektronické pošty mimo služební účely je považováno za vážné porušení pracovní kázně. Provoz elektronické pošty je monitorován.

Každý uživatel elektronické pošty má k dispozici schránku označenou standardizovaným jménem.

Elektronické poštovní schránky mohou být buď na jméno, nebo zástupné. Poštovní schránky na jméno smí užívat pouze ta fyzická osoba, pro kterou byla schránka vytvořena. Zástupné poštovní schránky reprezentují typ schránky, která má obecný charakter (např. podatelna, informace).

Lokální limity a omezení velikosti poštovních schránek pro uživatele elektronické pošty stanovuje provozovatel IS úřadu na základě technických možností.

Nebrání-li tomu objektivní skutečnosti, je uživatel povinen minimálně dvakrát v průběhu pracovní doby (jednou na počátku, jednou na konci) zkontrolovat svou elektronickou poštovní schránku. Pokud je to možné, musí uživatel odesílateli přijaté poštovní zprávy zaslat odpověď v jím požadovaném čase, nebo do dvou dnů.

Uživatel je povinen:

- vhodným způsobem minimalizovat velikost odesílané zprávy,
- neotvírat podezřelé soubory (přílohy), které mohou být nositeli viru nebo spamu a které mohou způsobit zavirování
- v případě zjištění, že se v některé přijaté zprávě nebo její části objevil počítačový virus, bezprostředně oznámit tuto skutečnost informatikovi-správci sítě.

- potvrdit vhodným způsobem převzetí došlé zprávy, je-li o to odesilatelem výslovně požádán,
- v případě očekávané nepřítomnosti pěti a více pracovních dnů nastavit ve schránce elektronické pošty pravidlo pro oznamování nepřítomnosti, po ukončení nepřítomnosti toto pravidlo odstranit,
- respektovat pokyny týkající se provozu elektronické pošty - neuposlechnutí pokynů je posuzováno jako hrubé porušení Provozního řádu IS úřadu.

Dostane-li uživatel zprávu, která obsahuje nevyžádané soubory, požádá informatika-správce sítě o kontrolu těchto souborů a o případné zpracování.

Provozovatel IS úřadu:

- je povinen zachovávat listovní tajemství všech uživatelů elektronické pošty,
- má právo zjistit důvod nadměrného počtu odesílaných a přijímaných zpráv v případě, že se tak děje dlouhodobě u některého z uživatelů,
- má právo zvýšit nebo omezit velikost elektronické pošty (emailové schránky) na základě požadavku nebo na základě porušení pravidel provozu elektronické pošty,
- je povinen informovat uživatele prostřednictvím intranetu, emailem nebo telefonem o výpadcích, změnách, instalacích, konfiguracích a nefunkčnosti elektronické pošty.

### 2.6.1. Postup v případě doručení úředního dokumentu, který podléhá evidenci

V případech kdy obsahem datové zprávy doručené do schránky elektronické pošty zaměstnanec je podání, které svým charakterem spadá do oblasti přímého výkonu veřejné správy (§ 1 zákona č.500/2004 Sb., správní řád), jde o podání, které podléhá evidenci.

Zaměstnanec, kterému byl doručen elektronický úřední dokument, který podléhá evidenci, je současně povinen neprodleně zaslat odesilateli „Potvrzení o doručení datové zprávy“.

## 2.7. Antivirová bezpečnost

Antivirová bezpečnost na úřadu je řešena jednotným softwarovým vybavením. Použití tohoto softwarového vybavení je závazné pro všechny organizační jednotky úřadu, není-li stanoveno jinak.

Antivirový software je nainstalován na všech počítačích úřadu, instalaci a konfiguraci software i jednotlivých úloh provádějí informatici-správci sítě.

Antivirovou kontrolu serverů zabezpečuje informatik-správce sítě.

Uživatel:

- je povinen dodržovat zásady antivirové bezpečnosti,
- nesmí měnit konfiguraci antivirového software,
- nesmí žádnou úlohu vypínat,
- je povinen bezprostředně oznámit pracovníkům odboru informatiky každý virový incident,
- je povinen kontrolovat antivirovým programem diskety, USB disky, paměťové karty, popř. jiná přenosná média a přílohy elektronické pošty

## 2.8. Internet

Internet je určen pouze pro služební účely. Využívání Internetu mimo služební účely je považováno za vážné porušení pracovní kázně. Provoz Internetu je monitorován.

Uživatel nese plnou odpovědnost za škody způsobené navštěvováním nevhodných internetových serverů (např. servery určené pro zábavu).

Správce IS si vyhrazuje právo v případě potřeby omezit uživatelům přístup k některým internetovým serverům).

## 2.9. Přístup mobilních uživatelů k IS úřadu

Smějí být používány pouze notebooky, PDA, kapesní PC a jiná mobilní zařízení umožňující drátové nebo bezdrátové připojení k síti zakoupené a poskytnuté prostřednictvím úřadu. Jakékoliv jiné mobilní zařízení, které bylo použito za účelem přenesení dat z jiné sítě, nebo je, popř. bylo připojeno k jiné síti, nesmí být do sítě úřadu připojeno.

Uživatelé mobilních zařízení jsou povinni kontrolovat správnou funkčnost antivirového programu, nesmějí instalovat jiné softwarové vybavení než to, které bylo instalováno provozovatelem IS.

Zavirování sítě IS způsobené nesprávným použitím mobilních zařízení se považuje za hrubé porušení provozního řádu IS.

Uživatel musí v co nejvyšší možné míře zamezit zcizení mobilních zařízení.

V případě závady, poruchy, ztráty či zcizení neprodleně tuto skutečnost oznámit odboru informatiky.

## 2.10. Vytváření přístupů uživatelů k IS úřadu

- Tajemník úřadu přijímá zaměstnance. Vedoucí odboru je povinen 7 dnů před nástupem nového zaměstnance do svého odboru vyplnit formulář „Požadavek na vytvoření přístupu k IS úřadu“ a podepsaný jej zaslat tajemníkovi, který jej předá informatikovi-správci sítě.



- Kancelář tajemníka úřadu informuje vedoucího odboru o podepsání pracovní smlouvy.
- Nově přijatý zaměstnanec je povinen prostudovat tento Řád provozování IS úřadu, kontaktovat lektora odboru informatiky a domluvit termíny úvodního zaškolení pro oblast informačních technologií.
- Budou-li splněny výše uvedené body, vytvoří odbor informatiky uživatelský účet a přístupová práva k požadovaným aplikacím.
- Vedoucí odboru je povinen zajistit aktualizaci telefonního seznamu.
- Nově přijatý zaměstnanec nesmí využívat IS úřadu bez dodržení výše uvedeného postupu.

## 2.11. Změna a rušení přístupů uživatelů k IS úřadu

- Dochází-li k převedení zaměstnance mezi odbory, nebo odděleními, nebo k odchodu zaměstnance, je nutné zajistit převod dat, souborů a přístupů k aplikacím.
- Pro tento účel je nutné, aby vedoucí příslušného odboru vyplnil formulář "Požadavek na zrušení přístupu a převod dat v IS úřadu", a to dostatečně včas tak, aby zaměstnanci odboru informatiky mohli tyto změny provést společně s převáděným – odcházejícím zaměstnancem. Vyplněný a podepsaný formulář musí být zaslán vedoucímu odboru informatiky, který zaeviduje datum převzetí a splnění požadavku.
- Nebude-li tento postup dodržen, nemůže odbor informatiky garantovat úplný převod dat a souborů mezi uživateli.

## 2.12. Publikování informací

Odbory úřadu jsou povinny publikovat nebo poskytovat pro publikování materiály a informace o své činnosti a o dění v městské části v rámci internetového a intranetového serveru.

Publikování informací v rámci internetového a intranetového serveru je řešeno tříúrovňovým systémem:

- a) zpracovatel – obvykle řadový pracovník odboru, který připravuje publikované materiály a informace,
- b) redaktor – obvykle vedoucí odboru, který schvaluje obsahovou stránku publikovaných materiálů a informací,
- c) šéfredaktor – pověřený pracovník odboru informatiky, který schvaluje formu a způsob publikování informací.

Odbory jsou povinni na požádání šéfredaktora zajistit právní dohled publikovaných materiálů a informací.

### 3. Závěrečná ustanovení

Pro uživatele správních a dopravně-správních evidencí Ministerstva vnitra (IISSE) pomocí vyhrazené výpočetní techniky platí „Zásady pro uživatele centrálního informačního systému“.

Tento Řád provozování IS úřadu nabývá účinnosti dnem .....

### 4. Přílohy

Příloha č. 1	Výkladový slovník IS úřadu
Příloha č. 2	Předávání dat IS úřadu
Příloha č. 3	Protokol pracoviště
Příloha č. 4	Požadavek na vytvoření přístupu k IS úřadu pro nově nastoupeného pracovníka
Příloha č.5	Požadavek na zrušení přístupu a převod dat v IS úřadu při personálních změnách