ORGANIZAČNÍ SMĚRNICE č. 11/21 PRAVIDLA UŽÍVÁNÍ PC, POČÍTAČOVÉ SÍTĚ, INTERNETU		Účinnost od: 23.8.2021
Zpracoval:	Ing. Tomáš Reichelt, tajemník Jakub Doležal – správce počítačové sítě	Datum vydání: 31.7.2021
Schválil:	Pavel Urx, starosta města Ing. Tomáš Reichelt, tajemník MěÚ	Revize č.: 0

Rozdělovník

Jméno	Funkce	Podpis
Pavel Urx	Starosta města	
Petr Jansa	Místostarosta města	
Ing. Tomáš Reichelt	Tajemník MěÚ	
Bc. Lenka Sluková	Vedoucí odboru FP	
Mgr. Zdeňka Čvančarová	Vedoucí odboru HS	
Ing. Irena Zárubová	Vedoucí odboru SÚ	
Ing. Petr Strnad	Vedoucí odboru MIŽP	

ORGANIZAČNÍ SMĚRNICE č. 11/21 PRAVIDLA UŽÍVÁNÍ PC, POČÍTAČOVÉ SÍTĚ, INTERNETU		Účinnost od: 23.8.2021
Zpracoval:	Ing. Tomáš Reichelt, tajemník Jakub Doležal – správce počítačové sítě	Datum vydání: 31.7.2021
Schválil:	Pavel Urx, starosta města Ing. Tomáš Reichelt, tajemník MěÚ	Revize č.: 0

Rozdělovník

Jméno	Podpis
Pavla Gerhardová	
Ivana Jandášová	
Věra Erlebachová	
Bc. Jitka Urgošová, DiS.	
Zdeňka Flídrová	
Kristýna Horká	
Bc. Jana Dolejšová, DiS.	
Monika Mansfeldová	
Andrea Dolejšová	
Jana Košková	
Barbora Flachsová	
Bc. Blanka Vyhnálková	
Ilona Bažantová	
Miroslav Vrabec	
Bc. Kamila Zárubová	

ORGANIZAČNÍ SMĚRNICE č. 11/21 PRAVIDLA UŽÍVÁNÍ PC, POČÍTAČOVÉ SÍTĚ, INTERNETU		Účinnost od: 23.8.2021
Zpracoval:	Ing. Tomáš Reichelt, tajemník Jakub Doležal – správce počítačové sítě	Datum vydání: 31.7.2021
Schválil:	Pavel Urx, starosta města Ing. Tomáš Reichelt, tajemník MěÚ	Revize č.: 0

Obsah

1. Působnost a účel organizační směrnice

1.1. Tato organizační směrnice slouží k zabezpečení bezporuchového užívání výpočetní techniky pro potřeby Městského úřadu Benešov nad Ploučnicí (dále jen „MěÚ").
1.2. Činnosti MěÚ jsou podporovány informačními a komunikačními technologiemi (dále také jen „ICT"), které jsou tvořeny na straně jedné hardwarem (počítače, notebooky, tablety, monitory, tiskárny, skenery, servery, aktivní síťové prvky, síťové rozvody, apod.) a na straně druhé softwarem (operační systémy, kancelářský software, aplikace, firewally, apod.). Spojením těchto technologií do konkrétní a funkční podoby v prostředí úřadu vzniká počítačová síť MěÚ (dále také jen „PS").
1.3. Tato organizační směrnice popisuje základní pravidla provozu a správy PS, upravuje závazný postup při používání zařízení, která jsou přímo připojena do PS a stanovuje základní povinnosti a pravomoci uživatelů a správce PS.
1.4. Organizační směrnice je závazná pro všechny zaměstnance MěÚ a všechna pracoviště MěÚ vybavená nebo používající počítačové prostředky.
1.5. Účelem směrnice je chránit MěÚ, uživatele, data uživatelů, data subjektů údajů, počítačové prostředky a PS před zneužitím a bezpečnostními incidenty.

2. Vymezení pojmů a zkratek

Aktivní síťový prvek – prvek sítě, který s datovým signálem vykonává určitou aktivní činnost
Aplikace – stejné jako software
EU – Evropská unie
GDPR – nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Hardware nebo HW – veškeré fyzicky existující technické vybavení informačních a komunikačních technologií
MěÚ – Městský úřad Benešov nad Ploučnicí
ICT – informační a komunikační technologie
Počítač – osobní počítač (PC – Personal Computer), notebook nebo tablet včetně všech svých periférií (monitor, klávesnice, myš, tiskárna, skener, apod.)
Pasivní síťový prvek – mechanická část sítě (kabely, spojky, rozvaděče, koncovky, zásuvky).
Počítačové prostředky – všechny prvky definované v kapitole 3.
Programové vybavení – stejné jako software
PS – počítačová síť
Software nebo SW – počítačový program získaný v souladu s obecně závaznými právními předpisy, zejména v souladu s autorským zákonem
Správce počítačové sítě (PS) – pan Jakub Doležal (ITEDO), IČ: 65117310
Subjekt údajů – identifikovaná nebo identifikovatelná fyzická osoba. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby (např. klient, zákazník, fyzická osoba podnikající, zaměstnanec, dítě, apod.)
Uživatel – osoba definovaná v kapitole 4., která používá PS MěÚ
Zástupce pro GDPR - určený zástupce pro problematiku GDPR

3. Počítačové prostředky

3.1 Server umístěný na vyhrazeném pracovišti spravovaný správcem PS a všechna periferní zařízení k němu připojená (např. diskové uložiště, zálohovací zařízení, bezpečnostní prvky, apod.).
3.2 Aktivní a pasivní síťové prvky.
3.3 Počítače na všech pracovištích MěÚ včetně přenosných počítačů (notebooků), tabletů a všech periferních a paměťových prvků připojených k těmto zařízením.
3.4 Síť optických kabelů, veřejný internet nebo ostatní zařízení pro datovou komunikaci (včetně mobilních telefonů připojených k PS MěÚ).
3.5 Tiskárny, plottery, skenery a multifunkční reprografické zařízení.
3.6 Veškeré softwarové vybavení serveru, aktivních síťových prvků, počítačů, apod.

4. Uživatel počítačových prostředků

Uživateli počítačových prostředků jsou:
a) zaměstnanci MěÚ, kteří potřebují a využívají ICT k plnění svých pracovních povinností,
b) správce PS,
c) jiné fyzické nebo právnické osoby, užívající počítačové prostředky vždy na základě požadavku a následného souhlasu správce PS a jím stanovených podmínek.

5. Přístup a používání počítačových prostředků

5.1 V počítačové síti MěÚ lze používat jen a pouze počítačové prostředky schválené správcem PS.
5.2 Počítačové prostředky jsou určeny pro použití pouze uživateli definovanými v kapitole 4. této směrnice.
5.3 Přístup k počítačovým prostředkům může být omezen, pokud budou počítačové prostředky přetíženy nebo v rámci řešení bezpečnostního incidentu (např. napadení PS MěÚ škodlivým kódem, porušení práv subjektu údajů, apod.).
5.4 Každý uživatel zároveň s tím, že pracuje (využívá počítačové prostředky) v PS MěÚ souhlasí s monitorováním své činnosti správcem PS, pokud vznikne podezření z porušování povinností, které jsou obsahem této směrnice. Monitorování činnosti uživatelů počítačových prostředků musí být prováděno vždy v souladu s platnou legislativou ČR, případně EU.
5.5 Správce PS je dále oprávněn, po odsouhlasení starostou města nebo tajemníkem MěÚ, spouštět software pro provádění pravidelného nebo náhodného bezpečnostního auditu PS MěÚ bez souhlasu uživatele (např. zjišťování nelegálního software; protiprávní stahování autorských děl; používání počítačových prostředků v rozporu s pracovní náplní uživatele, k soukromým účelům, nepovolené podnikatelské, komerční nebo trestní činnosti; apod.). Bezpečnostní audit musí být prováděn vždy v souladu s platnou legislativou ČR, případě EU.
5.6 Z provozních důvodů může správce PS omezit uživatelům využívané systémové zdroje (např. velikost e-mailové schránky, největší možná velikost odesílané přílohy, kvóta diskového prostoru, omezení připojení ke specifickým www adresám, omezení typu stahovaných souborů, apod.), o těchto opatřeních informuje tajemníka MěÚ.

6. Služby poskytované uživatelům

Uživatelům - zaměstnancům MěÚ jsou poskytovány tyto služby:

a) Výpočetní čas na počítačích spravovaných správcem PS, včetně přístupu k programovému vybavení zakoupenému k obecnému využití v PS MěÚ.
b) Elektronická pošta (e-mail), každý uživatel má nejméně jednu jednoznačnou adresu a má možnost doručovat a přijímat e-mail z IS TSML a.s. i veřejného internetu.
c) Uživatelská podpora k softwarovému vybavení zakoupenému k obecnému využití v PS MěÚ.
d) Interaktivní přístup do veřejného internetu.
e) Programová podpora spojená s provozem a instalací softwarového vybavení umožňující přístup a komunikaci se serverem PS MěÚ.
f) Správa a inovace počítačových prostředků.
g) Zřizování a rušení účtů uživatelům, jejich správu a údržba.
h) Zálohování všech dat uložených na serveru PS MěÚ (týká se pouze síťových disků).
i) Správa elektronických certifikátů (za bezpečnost přiděleného certifikátu odpovídá uživatel – zaměstnanec MěÚ).

7. Bezpečnostní incident

7.1 Bezpečnostní incident je situace, při které došlo k ohrožení bezpečnosti informací nebo k porušení definovaných pravidel. Bezpečnostní incident vzniká v důsledku selhání nebo nedodržení bezpečnostních opatření nebo porušení bezpečnostní politiky. Jako bezpečnostní incident může být vyhodnocený i pouhý neúspěšný pokus o nějaké zcizení nebo jiné znehodnocení informací. Při bezpečnostním incidentu může dojít k ohrožení, ztrátě, odcizení zneužití nebo změně počítačových prostředků, dat nebo informací.

7.2 Bezpečnostní incidenty jsou členěny podle závažnosti negativního vlivu na PS MěÚ a podle velikosti rizika spojeného s jeho dalším provozem:

a) Kritické bezpečnostní incidenty – jsou takové stavy počítačových prostředků, které brání provozu PS MěÚ, např. dlouhodobé plošné výpadky veřejného internetu, dlouhodobé výpadky databázových nebo aplikačních serverů, ztráta nebo krádež počítačových prostředků obsahující velké množství osobních údajů, apod.
b) Bezpečnostní incidenty vysoké závažnosti – jsou takové stavy počítačových prostředků, které mění funkčnost systému a významným způsobem ovlivňují nebo omezují práci uživatelů, např. nefunkčnost jednotlivých aplikací, hardwarové poruchy pracovních stanic uživatelů, apod.
c) Bezpečnostní incidenty střední závažnosti – jsou takové stavy počítačových prostředků, které dílčím způsobem mění nebo omezují funkčnost systému a ovlivňují práci uživatelů, např. nefunkčnost tiskárny, výměna klávesnice nebo myši, apod.
d) Bezpečnostní incidenty nízké závažnosti – jsou takové stavy počítačových prostředků, které mají jen lokálních charakter či jsou způsobeny uživatelskou chybou, např. uzamčení účtu uživatele, obnova smazaného dokumentu, apod.

7.3 Příklady bezpečnostních incidentů:

a) Krádež počítačových prostředků, dat nebo informací.
b) Ztráta počítačových prostředků, dat nebo informací.
c) Poškození počítačových prostředků, dat nebo informací.
d) Vloupání do kanceláře.
e) Neoprávněný přístup k datům nebo informacím.
f) Neoprávněné použití dat nebo informací.
g) Smazání dat nebo informací.
h) Selhání infrastruktury nebo připojení.

i) Selhání serveru, databáze nebo aplikace.
j) Hackerský útok, penetrace do IS TSML a.s..
k) Virový útok – škodlivý kód.
l) Útok ransomware.
m) Přírodní katastrofa.
n) Falšování webové stránky (spoofing).
o) Pokus o zcizení informací nebo dat., aj.

7.4 V případě, že uživatel zjistí, nebo je přímo účastníkem bezpečnostního incidentu, je povinen tuto skutečnost bezodkladně oznámit správci PS.

8. Ochrana osobních údajů

8.1 Uživatel je povinen plně dodržovat platnou legislativu ČR, případě EU v souvislosti s ochranou osobních údajů fyzických osob, zvláště pak ustanovení nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), v platném znění.

8.2 V případě, že uživatel zjistí, nebo je přímo účastníkem bezpečnostního incidentu porušení ochrany osobních údajů, je povinen tuto skutečnost bezodkladně oznámit zástupci pro GDPR. Bezpečnostním incidentem porušení ochrany osobních údajů se rozumí porušení zabezpečení osobních údajů představující riziko pro práva a svobody fyzických osob (ztráta kontroly nad osobními údaji, krádež či zneužití identity aj.) Podmínky, pravidla, procesní postupy ochrany osobních údajů jsou definovány v organizační směrnici města o ochraně osobních údajů (GDPR).

8.3 Při komunikaci se subjekty údajů nebo oprávněnými třetími stranami, kdy jsou obsahem komunikace osobní údaje, je uživatel povinen používat zabezpečených komunikačních prostředků jako je například: šifrovaný e-mail (pro hromadné předávání osobních údajů nebo zvláštní osobní údaje), datová schránka, zabezpečené uložiště, přílohy opatřené heslem, apod.

8.4 Uživateli je výslovně zakázáno pořizování kopií vedených osobních údajů libovolnou formou nad rámec jeho pracovní náplně a povinností.

8.5 Pokud jsou osobní údaje předávána třetí osobě, je povinností předávajícího uživatele vždy ověřit totožnost a oprávněnost osoby přebírající osobní data zpracovávat.

9. Poštovní schránky (e-mail)

9.1 Uživatel smí využívat poštovní schránky PS MěÚ pouze k činnostem souvisejícím s jeho pracovními povinnostmi nebo pracovní náplní.

9.2 Uživatelům je zakázáno přeposílat e-maily doručené do poštovních schránek PS MěÚ na své či jiné privátní (soukromé) poštovní schránky.

9.3 Prostřednictvím e-mailové komunikace je zakázáno posílání osobních údajů (GDPR) s výjimkou případů, kdy je použito šifrované komunikace či jsou osobní údaje zabezpečeny jiným způsobem (např. zipovaný soubor zabezpečený heslem, apod.).

10. Diskové uložiště – síťové disky

10.1 Data uložená na společném úložišti – síťovém disku jsou pravidelně (každou noc) zálohována. V případě potřeby je možné data uložená na tomto úložišti obnovit jeden měsíc zpětně.

10.2 Správce PS neodpovídá za ztrátu dat uživatelů uložených na lokálních discích počítačů, externích discích, paměťových kartách, flashdiscích, CD, DVD, apod.

11. Povinnosti uživatele

11.1 Uživatel se zavazuje, že nebude šířit a vědomě používat software získaný v rozporu s právními předpisy, zejména s autorským zákonem a že software, získaný v souladu s těmito předpisy nebude užívat v rozporu se smlouvou, kterou autor softwaru udělil svolení k jeho užití.
11.2 Uživateli je výslovně zakázáno používat počítačové prostředky neschválené správcem PS.
11.3 Uživatel nesmí instalovat jakýkoliv software bez vědomí správce PS.
11.4 V rámci PS MěÚ lze pracovat pouze s autorizovaným softwarovým vybavením, pro jehož provozování vlastní MěÚ licenční oprávnění, popř. s produkty, které byly vytvořeny na jeho základě.
11.5 Uživatel smí používat počítačové prostředky PS MěÚ pouze k činnostem daným jeho pracovními povinnostmi nebo pracovní náplní. Je výslovně zakázáno používat počítačové prostředky pro osobní, podnikatelské nebo komerční účely a k činnostem, které jsou v rozporu s platnou legislativou ČR, případě EU.
11.6 Uživatel je povinen do 15 pracovních dnů od účinnosti této směrnice zajistit u svého přiděleného PC případné odinstalování veškerého SW, který není uživatelem využíván v rámci jeho pracovní náplně, a to prostřednictvím správce PS, který odinstalování provede.
11.7 Uživatel smí využívat veřejný internet pouze k činnostem souvisejících s jeho pracovními povinnostmi nebo pracovní náplní.
11.8 Každý uživatel je zodpovědný za zabezpečení počítačových prostředků PS MěÚ proti zneužití (bezpečnostním incidentům) na svém pracovišti jemu dostupným možnostem (uzamčením místnosti, uzamknutím počítače, bezpečnými hesly viz dále, atd. ...).
11.9 Přístupová práva uživatele jsou dána jeho uživatelskou identifikací (přihlašovací jméno, heslo, případně další atributy sloužící k identifikaci uživatele). Uživatel se nesmí žádnými prostředky pokusit získat přístupová práva, která mu nebyla přidělena správcem PS. Pokud uživatel získá jemu nepřislušející přístupová práva jakýmkoli způsobem (včetně hardwarové nebo softwarové chyby systému), je povinen tuto skutečnost neprodleně ohlásit správci PS. Toto se vztahuje na všechny, ke kterým uživatel získá přístup pomocí počítačových prostředků. Uživatel se nesmí pokusit získat přístup k datům jiných uživatelů. Uživatel je dále povinen v rámci svých uživatelských práv maximálně zabezpečit svoje data proti zneužití třetími osobami.
11.10 Uživatel pracuje na počítačových prostředcích pouze pod uživatelským jménem jemu přiděleným správcem PS. Heslo ke svému uživatelskému jménu volí a udržuje v tajnosti tak aby bylo zabráněno jakékoliv možnosti zneužití. Uživatel zodpovídá za škody vzniklé v důsledku zneužití jeho účtu zaviněném nedbalou manipulací s účtem.
11.11 Uživatel nesmí pracovat pod uživatelským účtem jiného uživatele ani jej nesmí použít pro své přihlášení do systému a zároveň to nesmí umožnit ani jinému uživateli nebo třetí osobě.
11.12 Uživatel nesmí provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i případech, kdy tento uživatel svá vlastní data explicitně nechrání.
11.13 Uživatel je zodpovědný za posouzení nebezpečí zneužití přihlašovacích údajů a používání úměrně tomu bezpečných hesel. Uživatel je povinen dodržovat následující doporučení pro tvorbu hesla:
a) Nepoužívat uživatelské jméno, ani jeho přesmyčky nebo parafráze.

b) Nepoužívat žádné informace související s osobou uživatele (např. rodné číslo nebo jména uživatele, manžela (ky), přítele (kyně), dětí, psa, apod.).
c) Nepoužívat v heslech znaky s diakritikou.
d) Používat hesla o délce minimálně 10 znaků s výjimkou informačních systémů, které toto neumožňují.
e) Používat hesla, která budou obsahovat současně alespoň jedno malé písmeno, jedno velké písmeno, jednu číslici nebo jeden speciální znak (např. /, -, _, $, &, apod.) s výjimkou informačních systémů, které toto neumožňují).

11.14. Pro ochranu svých přihlašovacích údajů je uživatel povinen:
a) Nesdělovat svá hesla nikomu, ani svým nadřízeným.
b) Nezaznamenávat si hesla v žádné formě.
c) Odhlašovat se ze systému vždy, když nemůže zajistit nezneužití počítačových prostředků jinou osobou (bezpečnostní incident).
d) Při zadávání hesla nepřipustit odpozorování hesla jinou osobou.
e) Pokud má uživatel podezření, že bylo heslo prozrazeno a mohlo by dojít ke zneužití počítačových prostředků PS MěÚ (bezpečnostní incident), provede bezodkladně všechny potřebné úkony pro změnu hesla.

11.15 Pokud je z provozních důvodů nutné, aby více uživatelů sdílelo osobní údaje, je nutný písemný souhlas všech dotčených uživatelů (subjektů údajů).

11.16 Uživatel plně zodpovídá za škody vzniklé zneužitím jeho přístupového oprávnění (jména - loginu a hesla) k počítačovým prostředkům PS MěÚ.

11.17 Je zakázáno kopírovat a distribuovat části operačního systému a nainstalovaných aplikací a software. Programy je možné používat jen na takovou činnost, na kterou jsou určené.

11.18 Uživateli není dovolena neautorizovaná modifikace programů, dat nebo technického vybavení počítačů patřící pod PS MěÚ. Zvlášť přísně jsou pak zakázány neautorizované změny počítačových prostředků, které by mohly mít vliv na provoz celého PS MěÚ.

11.19 Bez souhlasu správce PS není uživatel oprávněn přemísťovat počítačové prostředky a odpojovat kabely. Toto omezení neplatí pro přenosné počítačové prostředky (notebooky, dataprojektory, tablety, apod.).

11.20 Uživatel nesmí jakýmkoliv způsobem zasahovat do PS MěÚ, kromě výměny spotřebního materiálu u tiskových a multifunkčních reprografických zařízení (tzn. papíru, papírových kotoučů, barvící pásky, toneru nebo inkoustu, apod.).

11.21 Uživatel nesmí měnit mapování a sdílení disků vytvořených správcem PS.

11.22 Uživatel je povinen pracovat s počítačovými prostředky tak, aby je nepoškodil, zejména mechanicky. Uživatel nemá oprávnění k rozebírání počítačových prostředků včetně odstraňování krytu.

11.23 Při přerušení práce se ztrátou dohledu nad počítačem (i při krátkodobém opuštění pracoviště) je uživatel povinen dostatečným způsobem zabránit neoprávněnému použití počítačových prostředků, např. uzamknutím počítače v případě opuštění kanceláře (Ctrl+Alt+Del s následným výběrem volby Uzamknout počítač), při delší absenci a při odchodu z pracoviště domů vypnout PC standardním způsobem (přes tlačítko START, popřípadě přes ikonu napájení).

11.24 V případě nutných udržovacích či servisních pracích prováděných správcem PS na PC jednotlivých uživatelů po pracovní době je na základě předchozí informace správce PS o tomto kroku uživatel povinen ponechat PC v provozu, tzn. nevypínat ho.

11.25 V případě potřeby přístupu k datům nepřítomného uživatele je nutné zajistit souhlas tajemníka MěÚ a daného nepřítomného uživatele k této operaci a kontaktovat správce MěÚ, který následně zajistí zpřístupnění dat žadateli.

11.26 V PS MěÚ je nainstalován antivirový program, který zabezpečuje antivirovou kontrolu souborů počítačů a elektronické pošty, včetně jejich příloh. Program vytváří na každém počítači rezidentní štít, který brání vniknutí a šíření škodlivého kódu do počítače. Antivirová databáze je prostřednictvím PS MěÚ aktualizována. Uživatel nesmí přerušovat aktualizaci antivirového prostředku a je povinen se řídit pokyny antivirového programu, především pokynu pro opětovné spuštění (restart) počítače. Stejné nařízení je platné i pro aktualizace operačního systému počítače.

11.27 Napadení počítače nebo serveru škodlivým kódem (různé formy počítačových virů) zapříčiněné svévolným počínáním uživatele v rozporu s ustanoveními této organizační směrnice, resp. nedbalostí je považováno v souladu s pracovním řádem za porušení pracovní kázně.

11.28 Pokud uživatel zjistí nebo je přímo účastníkem bezpečnostního incidentu (např. napadení počítače škodlivým kódem; ztráta nebo krádež počítačových prostředků, informací nebo dat, apod.) je povinen okamžitě přerušit práci na počítačových prostředcích a neprodleně prokazatelným způsobem informovat správce PS o bezpečnostním incidentu.

11.29 V blízkosti počítačů je zakázáno jíst, pít a kouřit, nebo provádět činnosti, které vedou ke znečištění prostředí. Manipulovat s otevřeným ohněm a hořlavinami, jakož i s těkavými látkami, kyselinami a rozpouštědly.

11.30 Dále je zakázáno manipulovat s rozvodem elektrické energie a s kabeláží počítačových prostředků kromě osob k tomu určených.

11.31 Do zásuvek speciálního silnoproudého rozvodu je zakázáno zapojovat jiné spotřebiče než prvky počítačových prostředků.

12. Povinnosti správce PS

12.1 Správce PS je povinen chránit data uživatelů a nakládat s nimi tak, aby nedošlo k jejich odhalení nebo zneužití.

12.2 S výjimkou plnění svých pracovních povinností nesmí prohlížet obsah nebo kopírovat jakákoliv data nebo programy z uživatelských adresářů bez výslovného souhlasu jejich majitele (uživatele).

12.3 Bez prokazatelného souhlasu kompetentního uživatele nesmí předat data (zvláště pak osobní data subjektů údajů) třetí straně.

12.4 Je povinen včas informovat uživatele o výpadcích PS MěÚ.

12.5 Odpovídá za instalování softwaru v souladu s licenčními nebo smluvními podmínkami a zajišťuje kontrolu dodržování pravidel pro používání softwaru.

12.6 Servisní zásahy na PC uživatele pomocí vzdáleného přístupu v pracovní době uživatele v případě jeho přítomnosti realizuje jen s předchozím odsouhlasením (telefonicky, e-mailem) uživatele.

13. Pravidla komunikace v PS MěÚ

13.1 Je zakázáno používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším uživatelům (elektronické diskusní skupiny, e-mail, zprávy, aj.).

13.2 Je zakázáno využívat počítačových prostředků (především elektronické pošty) k obtěžování nebo zastrašování jiných uživatelů. Dále je zakázáno používat počítačových prostředků pro šíření obchodních informací, politickou nebo náboženskou propagaci a šíření materiálů, které jsou v rozporu s právními předpisy. Rovněž je zakázáno obtěžování ostatních uživatelů hromadnými zprávami a zprávami, které svým charakterem nesouvisí přímo s pracovním zařazením a povinnostmi.

13.3 Je zakázáno zneužívat počítačových prostředků k reklamním a jiným účelům, sloužícím k získání osobního prospěchu.
13.4 Je zakázáno používat počítačové prostředky k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím PS MěÚ.
13.5 Uživatel je povinen dodržovat, aby jeho činnost jen v minimálním rozsahu negativně ovlivňovala možnosti využití počítačových prostředků dalšími uživateli. To se týká jak neúměrného zatěžování linek v době jejich maximálního využití, tak i neúměrného zatěžování jednotlivých počítačů. Všechny takovéto činnosti je vhodné konzultovat se správcem PS a řídit se jeho pokyny.
13.6 Velikost přílohy elektronické pošty by neměla přesáhnout 20 MB. Správce PS má právo systémově omezit velikost příloh.
13.7 Uživatel není oprávněn využívat nedovoleným způsobem data uložená v PS MěÚ, systémy a počítačové prostředky nebo neoprávněně zkoušet, zkoumat nebo testovat zranitelnost těchto systémů.

14. Sociální sítě

14.1 Sociální síť, zvaná též společenská síť, komunitní síť nebo komunita, anglicky „social network", je propojená skupina lidí. Pro potřeby této směrnice je sociální sítí chápána služba na veřejném internetu, která registrovaným členům umožňuje si vytvářet osobní (nebo firemní) veřejný nebo částečně veřejný profil, komunikovat spolu, sdílet informace, fotografie, videa, provozovat chat a další aktivity (např. Facebook, Twitter, Instagram, Lidé, LinkedIn, MySpace, Líbímseti, Google Plus, YouTube, Lidé, Skype, ICQ, apod.). Komunikace mezi uživateli sociálních sítí může probíhat mezi dvěma uživateli nebo (nejčastěji) hromadně mezi uživatelem a skupinou s ním propojených dalších uživatelů.
14.2 Uživateli je zakázáno v rámci PS MěÚ používat sociální sítě nebo jakýmkoliv jiným způsobem přispívat nebo využívat služeb sociálních sítí.
14.3 Uživateli je zakázáno v rámci sociálních sítí vytvářet (zakládat) uživatelské účty nebo profily jménem MěÚ. Tato povinnost se vztahuje komplexně na činnosti pracovního i soukromého charakteru, na pracovní i mimopracovní dobu uživatele.
14.4 V případě, že uživatel k plnění svých pracovních povinností nezbytně potřebuje založit na sociální síti účet nebo profil jménem MěÚ, může tak učinit pouze s výslovným souhlasem starosty města nebo tajemníka MěÚ.
14.5 V případě, že uživatel k plnění svých pracovních povinností nezbytně potřebuje využívat služeb sociální sítě, může tak učinit pouze s výslovným souhlasem starosty města nebo tajemníka MěÚ.

15. Uživatelská podpora (požadavky, řešení havarijních stavů, apod.)

15.1 Uživatelé předávají veškeré požadavky na uživatelskou podporu správce PS na kontakty: tel. 602 759 725, 604 117 186, e-mail: dolezal@itedo.cz, vesely@itedo.cz
15.2 Pracovní doba uživatelské podpory je zajištěna v:
pondělí - pátek: od 8:00 do 17:00 hodin.

16. Uchovávání dat a médií

16.1 Uživatelé uchovávají svá pracovní data v adresářích (složkách) na síťových discích. R: data, M: scan, I: install, atd..

16.2 Lokální disky počítačů nejsou určeny pro ukládání pracovních dat. V případě, že uživatel uchovává data na lokálních discích, externích discích, CD médiích, DVD médiích, flashdiscích, paměťových kartách, apod., odpovídá plně za zabezpečení svého datového fondu. Za takto umístěná data nenese správce PS žádnou odpovědnost.
16.3 Uživateli je povoleno na síťových i lokálních discích uchovávat pouze data, která bezprostředně souvisí s jejich pracovní náplní nebo činností.

17. Úkony při ukončení pracovního poměru

17.1 Při ukončení pracovního poměru je uživatel povinen předat svůj osobní pracovní adresář umístěný na síťovém disku svému nástupci nebo příslušnému nadřízenému.
17.2 Při ukončení pracovního poměru je uživatel povinen předat svoji poštovní schránku svému nástupci nebo příslušnému nadřízenému.
17.3 Při ukončení pracovního poměru je uživatel povinen předat veškerou svou pracovní elektronickou agendu (aplikační data, dokumenty umístěné ve společných složkách/adresářích, apod.) svému nástupci nebo příslušnému nadřízenému.
17.4 U uživatele, který končí pracovní poměr, odpovídá příslušný nadřízený za předání veškeré elektronické agendy (e-mailová komunikace, ekonomický systém, aplikační data, dokumenty umístěné v osobních i společných složkách/adresářích, apod.) svému nástupci nebo jím určenému uživateli.
17.5 Při ukončení pracovního poměru je uživatel povinen předat svěřený počítač vč. příslušenství správci PS. U uživatele, který končí pracovní poměr, oznámí tuto skutečnost příslušný nadřízený správci PS v dostatečném předstihu (min. 3 pracovní dny předem). Správce PS převezme počítač včetně příslušenství od uživatele, provede kontrolu jeho funkčnosti a stavu a zaeviduje jeho nové umístění. V případě vrácení počítače včetně příslušenství v poškozeném nebo neúplném stavu informuje správce PS příslušného nadřízeného nebo tajemníka MěÚ.
17.6 U uživatele, který končí pracovní poměr a současně vlastní kvalifikovaný (QCA) nebo komerční (VCA) certifikát, musí být správcem PS vždy potvrzeno zneplatnění tohoto/těchto certifikátu/ů. V případě, že uživatel má zapůjčen token, je povinen tento token protokolárně vrátit správci PS.

18. Porušení směrnice a sankce

18.1 Administrátor nebo správce má právo zrušit (ukončit) přístup k počítačovým prostředkům uživatelů, kteří prokazatelně porušili ustanovení této organizační směrnice, a to na dobu potřebnou k novému definování přístupových práv příslušným nadřízeným.
18.2 V případě porušení této organizační směrnice mohou být uplatněny sankce podle obecně závazných právních předpisů, případně jiných interních předpisů MěÚ (pracovního řádu, apod.).
18.3 Porušení této směrnice je považováno za hrubé porušení pracovní kázně uživatele.

19. Požadované základní dovednosti uživatele

19.1 Všichni uživatelé jsou povinni ovládat počítačové prostředky PS MěÚ, potřebné pro výkon jejich pracovní náplně nebo pracovních povinností v rámci uživateli přidělené pracovní pozice.
19.2 Základní funkce a aplikace:
a) operační systém MS Windows
b) kancelářský software MS (Word, Excel, Outlook)

c) veřejný internet
d) aplikace potřebné pro výkon pracovní pozice.

19.3 V rámci přijímacího řízení je vždy u nového potencionálního uživatele ověřena úroveň počítačových dovedností.