STATUTÁRNÍ MĚSTO LIBEREC

Poznámka: *Zveřejněna je pouze upravená verze dokumentu z důvodu dodržení přiměřenosti rozsahu zveřejňovaných osobních údajů podle nařízení Evropského parlamentu a rady (EU) 2016/679 , 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 a aplikačních zákonů ČR).*
Nejsou dotčena práva podle § 16 odst. 2 písm. e) zákona č. 128/2000 Sb., o obcích (obecní zřízení) oprávněných osob uvedených v § 16 a § 17 téhož zákona.

14. schůze rady města dne: 16.06.2020

Bod pořadu jednání: 87

Směrnice 21RM – Provoz informačního systému SML

Stručný obsah: Schválení nové směrnice RM – Provoz informačního systému statutárního města Liberec (dále jen "Provoz IS SML"). Nová směrnice nahrazuje aktuální směrnici tajemníka 12T Provoz IS MML. Nová směrnice aktualizuje pravidla a procesy týkající se provozu IS SML zvláště s ohledem na aktuální požadavky na bezpečnost informačních systémů (ochrana osobních údajů, nástupy a výstupy, bezdrátové připojení k IS SML, apod.).

MML, Odbor vnitřních věcí

Důvod předložení: Vydání směrnice RM - Provoz informačního systému SML

Zpracoval: Vavřina Zbyněk, Ing. - vedoucí odboru vnitřních věcí

Projednáno s: Ing. Martinem Čechem, tajemníkem MML

na poradě vedení dne 25.5.2020

Předkládá: Vavřina Zbyněk, Ing. - vedoucí odboru vnitřních věcí

K projednání v radě přizván(a):

Předpokládaná doba projednání (min): 10

Po schválení předložit na jednání:

Návrh usnesení

Rada města po projednání

vydává

novou směrnici rady č. 21RM Provoz informačního systému statutárního města Liberec s účinností od 1. 7. 2020.

ukládá

seznámit všechny zaměstanance statutárního města Liberec a uvolněné členy zastupitelstva města Liberec s obsahem nové směrnice č. 21RM Provoz informačního systému statutárního města Liberec.

P: Čech Martin, Ing. - tajemník Magistrátu města Liberec
T: 23.06.2020

Důvodová zpráva

Schválení nové směrnice č. 21RM - Provoz informačního systému statutárního města Liberec (dále jen "Provoz IS SML"). Nová směrnice nahrazuje aktuální směrnici tajemníka 12T Provoz IS MML. Nová směrnice aktualizuje pravidla a procesy týkající se provozu IS SML s ohledem na aktuální požadavky na bezpečnost informačních systémů provozovaných v prostředí statutárního města Liberec (ochrana osobních údajů, nástupy a výstupy, bezdrátové připojení k IS SML, apod.).

Směrnice byla představena a diskutována na poradě vedení dne 25. 5. 2020 s kladným hodnocením.

Popis změn nové směrnice RM:

1) Změna rozsahu působnosti směrnice, nyní: zaměstnanci, uvolnění členové zastupitelstva, DPP, DPČ, obchodní smlouva, jiná fyzická osoba.

2) Konkrétnější popis povinnosti chránit počítačové prostředky.

3) Způsob komunikace vně IS SML - práce s cloudem: https://cloud.liberec.cz/.

4) Úprava pravidel v oblasti ochrany osobních údajů.

5) Úprava definice "klíčového uživatele".

6) Zahájení pracovního vztahu uživatele (přesun), ukončení pracovního vztahu.

7) Požadavky na SW instalovaný do prostředí IS SML.

8) Bezdrátové připojení do IS SML.

9) Používání sociálních sítí.

Přílohy:
21RM_Smernice_Provoz_IS_SML_20200608

Liberec: 8.6.2020

Účinnost od: 1.7.2020

STATUTÁRNÍ MĚSTO LIBEREC

Směrnice rady č. 21RM

Provoz informačního systému statutárního města Liberec

	Jméno a příjmení	Datum
Zpracoval	Ing. Zbyněk Vavřina	8.6.2020
Odsouhlasil	Ing. Martin Čech	8.6.2020
Schválil	Usnesení RM č. XXX	16.6.2020

Obsah

1. Úvodní ustanovení

Rada města Liberec, příslušná podle § 102 odst. 3 zákona č. 128/2000 Sb., o obcích, vydává následující vnitřní právní předpis.

2. Působnost a účel směrnice

1. Vlastní provoz činností statutárního města Liberec (dále jen SML) je podporován z velké části informačními a komunikačními technologiemi (dále také ICT). Tyto ICT jsou tvořeny hardwarem (např. počítače, notebooky, tablety, monitory, tiskárny, skenery, servery, aktivní prvky, síťové rozvody, mobilní telefony, apod.) a SW (např. operační systémy, kancelářský software, aplikace – agendové informační systémy, firewally, apod.). Spojením HW a SW do konkrétní a funkční podoby v prostředí SML vzniká to, co se nazývá Informační systémem statutárního města Liberec (dále také IS SML).
2. Směrnice „Provoz informačního systému statutárního města Liberec“ (dále také směrnice) popisuje základní pravidla provozu a správy IS SML, upravuje závazný postup při používání počítačových prostředků, která jsou přímo připojena do IS SML a definuje základní povinné počítačové dovednosti uživatele.
3. Směrnice je závazná pro všechny zaměstnance SML (s výjimkou zaměstnanců Městské policie Liberec), uvolněné členy Zastupitelstva města Liberec a fyzické osoby vykonávající činnosti pro SML v rámci odborné praxe nebo stáže na všech pracovištích SML.
4. Provozovatelem IS SML je odbor vnitřních věcí.
5. Účelem směrnice je chránit SML, uživatele, data uživatele, data subjektů údajů, data klientů, počítačové prostředky a IS SML před zneužitím a bezpečnostními incidenty.

3. Vymezení pojmů a zkratek

Administrátor IS – vedoucí odboru vnitřních věcí nebo jím pověřený zástupce, zaměstnanec oddělení informatiky a řízení procesů nebo pracovník Liberecké IS, a. s. zajišťující provoz a správu počítačových prostředků informačního systému statutárního města Liberec.

Aktivní síťový prvek - aktivní síťový prvek, opak pasivního prvku sítě, je takový prvek sítě, který s datovým signálem vykonává určitou aktivní činnost (např. opakovač, rozbočovač, most, tiskový server, brána, přepínač, apod.).

Aktivně využívaná služba IS SML – počítač nebo mobilní zařízení je připojené do IS SML pevným nebo bezdrátovým způsobem a současně se uživatel přihlásí do IS SML svým doménovým účtem.

Aplikace – blíže viz „Software nebo SW“.

Data – informace uložená v počítačových prostředcích (např. databáze, dokument, soubor, e-mail, hesla, uživatelské účty, konfigurace, záznam o činnost – log, apod.)

EU – Evropská unie.

Externí paměťová média – paměťové karty, externí pevné disky, flash disky, CD, DVD, apod.

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).

GIS – geografický informační systém – je počítačový systém, který umožňuje ukládat, spravovat a analyzovat prostorová data.

Hardware nebo HW – veškeré fyzicky existující technické vybavení informačních a komunikačních technologií.

HelpDesk – SW nástroj určený k řízení procesů spojených s řešením požadavků v oblasti ICT (evidence požadavků, sledování jejich stavu a historie).

Hosting – je pronájem ICT prostoru (HW, SW, komunikační trasy včetně doprovodných služeb) pro provoz aplikací, webu či jiné služby na cizích ICT prostředcích. Pronajímatel ICT prostředků bývá označován jako poskytovatel hostingu.

ICT – informační a komunikační technologie.

IS – informační systém.

IS SML – informační systém statutárního města Liberec.

ISEO – informační systém evidence obyvatel.

ISZR – informační systém základních registrů.

KASRO – společnost Kasro, s. r. o. – poskytovatel reprografických služeb.

LIS – společnost Liberecká IS, a. s. – poskytovatel ICT služeb.

MML – Magistrát města Liberec.

Mobilní zařízení – mobilní telefon nebo tablet ve všech jeho technologických variantách a včetně všech svých periférií (klávesnice, tiskárna, paměťová karta, flashdisk, externí pevný disk, dataprojektor, apod.) připojených k tomuto zařízení. Do této kategorie není započítáván notebook.

Odbor – organizační jednotka MML, definovaná směrnicí RM č. 1RM – Organizační řád.

Pasivní síťový prvek – pasivní síťový prvek, je takový prvek sítě, který fyzicky zajišťuje přenos dat v síti. Zjednodušeně lze říci, že je to především kabeláž a všechny nutné prvky kolem (např. zásuvky, spojky, kabeláž, apod.).

Počítač – osobní počítač (PC – Personal Computer), VDI nebo notebook ve všech jeho technologických variantách a včetně všech periférií (monitor, klávesnice, myš, tiskárna, skener, paměťová karta, flashdisk, externí pevný disk, apod.) připojených k tomuto zařízení.

Počítačové prostředky – všechny prvky definované v kapitole 4.

Právní předpis – právní předpis je pramen práva, označovaný také jako normativní právní akt, který je jednostranně vydán orgánem veřejné moci a který obsahuje jednu, zpravidla ale více právních norem jako obecně závazných pravidel chování nebo jejich složek. Protože jde vždy o písemný dokument, z hlediska typu jako pramen práva tvoří psané právo. Právní předpisy jsou součástí právního řádu a navzájem se hierarchicky strukturují především podle své právní síly.

Pracovní vztah – pracovní poměr, nebo právní vztahy, založené dohodami o pracích konaných mimo pracovní poměr.

Server – je obecné označení pro počítač, který poskytuje nějaké služby, nebo počítačový program, který tyto služby realizuje včetně všech periferních zařízení k němu připojených (např. diskové uložiště, zálohovací zařízení, bezpečnostní prvky, zdroj náhradního napájení, apod.). V unixových systémech je případně označován jako démon (anglicky daemon), v Microsoft Windows potom jako služba (anglicky service).

SML – statutární město Liberec.

Sociální síť – 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 vytvářet si osobní (nebo firemní) veřejný nebo částečně veřejný profil, komunikovat spolu, sdílet data, fotografie, videa, provozovat chat a další aktivity (např. Facebook, Twitter, Instagram, Lidé.cz, LinkedIn, MySpace, Líbímseti, GooglePlus, YouTube, Skype, ICQ, apod.). Komunikace na sociálních sítích může probíhat mezi dvěma osobami nebo (nejčastěji) hromadně mezi osobou a skupinou s ním propojených dalších osob.

Software nebo SW – sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. Software lze rozdělit na systémový software, který zajišťuje chod samotného počítače a jeho styk s okolím a na aplikační software (dále také aplikace), se kterým pracuje uživatel počítače.

Správce IS – vedoucí odboru vnitřních věcí či jeho pověřený zástupce.

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.

Uživatel – osoba užívající autorizované i neautorizované počítačové prostředky.

VDI – (Virtual Desktop Infrastructure) – počítač běží virtualizovaně na serverech IS SML, zatímco je ovládán z koncového klientského zařízení.

VV – odbor vnitřních věcí.

VVOI – oddělení informatiky a řízení procesů.

WIFI nebo bezdrátová počítačová síť – je typ počítačové sítě, ve které je spojení mezi jednotlivými uživateli sítě uskutečňováno pomocí bezdrátové komunikace.

4. Počítačové prostředky

V rámci IS SML jsou počítačové prostředky rozděleny do dvou kategorií:

1. Autorizované počítačové prostředky – počítačový prostředek spravovaný administrátorem IS a současně schválen správcem IS:
   a) Servery umístěné na vyhrazených pracovištích IS SML.
   b) Aktivní a pasivní síťové prvky.
   c) Počítače připojené do IS SML.
   d) Mobilní zařízení připojené do IS SML.
   e) Veškeré SW vybavení serverů, aktivních prvků, počítačů a mobilních zařízení.
   f) Veškerá data uložená v IS SML.
   g) Veřejný internet dostupný z IS SML.
   h) Síť optických kabelů (MAN).
   i) Tiskárny, plottery, skenery a multifunkční reprografické zařízení firmy KASRO.
   j) Provoz aplikací či služeb zajišťovaných formou hostingu.
2. Neautorizované počítačové prostředky – počítačový prostředek není spravován administrátorem IS a nebyl schválen správcem IS:
   a) Hardware.
   b) Software.
   c) Data.

   Jako příklad lze uvést soukromé počítačové prostředky zaměstnanců, uvolněných členů Zastupitelstva města Liberec nebo fyzických osob vykonávající činnosti pro SML v rámci odborné praxe (mobilní telefony, tablety, notebooky, apod.), mobilní telefony či počítače dodavatelů, hostů, apod.

5. Uživatel autorizovaných počítačových prostředků

Uživatelem autorizovaných počítačových prostředků může být pouze:

1. Zaměstnanec SML v hlavním pracovním poměru (s výjimkou zaměstnance Městské policie Liberec), který potřebuje a využívá ICT k plnění svých pracovních povinností.
2. Zaměstnanec SML vykonávající činnosti pro SML na základě uzavřené dohody o pracovní činnosti nebo dohody o provedení práce, vždy na základě požadavku zadaného vedoucím příslušného odboru nebo tajemníkem MML na HelpDesk a následného posouzení a případného povolení správcem IS dle definovaných pravidel touto směrnicí.
3. Uvolněný člen Zastupitelstva města Liberec.
4. Administrátor IS.

5. Správce IS.
6. Fyzická osoba vykonávající činnosti pro SML v rámci odborné praxe nebo stáže, vždy na základě požadavku zadaného tajemníkem MML na HelpDesk a následného posouzení správcem IS dle definovaných pravidel touto směrnicí.
7. Právnická osoba vykonávající činnosti správy IS SML (např. technická podpora aplikací, technologického centra, MAN, apod.) nebo jiných technologických zařízení provozovaných v prostředí SML (např. kamerový systém, parkovací systém, kogenerační jednotky, kremační pece, apod.) na základě uzavřené a platné obchodní smlouvy, a vždy se souhlasem administrátora IS a správce IS.

6. Informační systém statutárního města Liberec

Informační systém statutárního města Liberec je souhrn všech počítačových prostředků, ve všech objektech SML i mimo ně, sloužících k podpoře a řízení procesů statutárního města Liberec, manažerského rozhodování a správě provozovaných aplikací. IS SML je rozdělen do dvou instancí:

1) IS SML NEVEŘEJNÝ – pro připojení do neveřejné instance informačního systému statutárního města Liberec mohou být použity pouze autorizované počítačové prostředky a k jejich připojení je možno použít:
   a) Pevné připojení (kabel).
   b) Bezdrátové připojení (WIFI) prostřednictvím sítě „MML“.
   c) Veřejný internet, pouze v případě vzdáleného připojení.
2) IS SML VEŘEJNÝ – veřejný informační systém statutárního města Liberec poskytuje pouze jednu službu a tou je připojení do veřejného internetu. Do veřejného informačního systému statutárního města Liberec mohou být připojeny autorizované i neautorizované počítačové prostředky a k jejich připojení je možno použít pouze:
   a) Bezdrátové připojení (WIFI) prostřednictvím sítě „MML-hoste“.
   b) Bezdrátové připojení (WIFI) prostřednictvím sítě „MML-RMZM“.
   c) Bezdrátové připojení (WIFI) prostřednictvím sítě „MestoLiberec“.

7. WIFI – bezdrátové připojení do IS SML

V rámci IS SML jsou provozovány následující bezdrátové sítě:

1) MML – bezdrátové připojení do neveřejné instance IS SML. Je určeno pouze pro uživatele autorizovaných počítačových prostředků a to konkrétně pouze počítačů. Přístup k síti je zabezpečen.
2) MML-hoste – bezdrátové připojení do veřejné instance IS SML. Je určeno pro připojení autorizovaných i neautorizovaných počítačových prostředků. Přístup k síti je zabezpečen.

3) MML-RMZM – bezdrátové připojení do veřejné instance IS SML. Je určeno pro připojení autorizovaných i neautorizovaných počítačových prostředků. Tuto síť mohou využívat pouze zastupitelé statutárního města Liberec a je určena pouze k vykonávání činností spojených s výkonem funkce zastupitele.

4) MestoLiberec – bezdrátové připojení do veřejné instance IS SML. Je určeno pro připojení neautorizovaných počítačových prostředků. Tuto síť, která je dostupná v lokalitě náměstí před historickou budovou Radnice, může využívat široká veřejnost. Přístup k síti není zabezpečen.

8. Dostupnost IS SML a používání počítačových prostředků

1. Přístup do IS SML je možný 24 hodin 7 dní v týdnu s výjimkou předem oznámených odstávek IS SML.
2. Odstávky IS SML jsou vždy včas oznámeny uživateli. Za informování uživatele je odpovědný administrátor IS.
3. Přístup k počítačovým prostředkům může být omezen, pokud jsou počítačové prostředky přetíženy nebo v rámci řešení bezpečnostního incidentu (např. napadení IS SML škodlivým kódem, porušení práv subjektu údajů, apod.).
4. Uživateli není umožněn administrátorský přístup k autorizovaným počítačovým prostředkům.
5. V IS SML NEVEŘEJNÝ lze používat jen a pouze autorizované počítačové prostředky.
6. Uživatel využívající počítačové prostředky může být počítačově monitorován. Počítačový monitoring může být proveden pouze za předpokladu splnění podmínky oprávněného zájmu SML. Administrátora IS oprávněného k monitorování a objekt monitorování určuje primátor SML společně s tajemníkem MML a správcem IS. Monitorování činnosti uživatele počítačových prostředků musí být prováděno vždy v souladu s právními předpisy. Do 14 (čtrnácti) pracovních dnů od vyhodnocení monitorování uživatelů bude správcem IS předložena zpráva do porady vedení.
7. Administrátor IS se souhlasem správce IS je oprávněn provádět audity IS SML (např. v případě bezpečnostního incidentu; zjišťování nelegálního SW; protiprávní stahování autorských děl; používání počítačových prostředků v rozporu s pracovní náplní uživatele či touto směrnicí; používání pracovních prostředků k soukromým účelům, nepovolené podnikatelské, komerční nebo trestní činnosti; inventarizaci; apod.). Audit musí být prováděn vždy v souladu s právními předpisy.
8. Z provozních důvodů může administrátor IS omezit uživateli využívané systémové zdroje (např. velikost e-mailové schránky, největší možná velikost odesílané přílohy, kvóta diskového prostoru, omezení připojení ke specifickým URL adresám, omezení typu stahovaných souborů, apod.), avšak pouze se svolením správce IS. V případě výjimek z těchto omezení je třeba zadat na HelpDesk požadavek vedoucím příslušného odboru uživatele.

9. Nákup mobilního zařízení, u kterého je požadováno připojení do IS SML NEVEŘEJNÝ, podléhá vždy projednání se správcem IS. Správce IS schválí pouze nákup mobilního zařízení, které je kompatibilní pro používání v IS SML NEVEŘEJNÝ. Pokud bude uživatelem zakoupeno neschválené mobilní zařízení, nenese za jeho funkčnost v IS SML NEVEŘEJNÝ správce IS žádnou odpovědnost a může být administrátorem IS odmítnuto takovéto mobilní zařízení připojit do IS SML NEVEŘEJNÝ. Zprovoznění mobilního zařízení v prostředí IS SML NEVEŘEJNÝ je prováděno vždy administrátorem IS.
10. Uživateli je výslovně zakázáno poskytnutí autorizovaného počítačového prostředku neoprávněné osobě (např. rodinnému příslušníkovi, obchodnímu partnerovi, apod.) k jakémukoliv užití.
11. Uživatel smí používat autorizované počítačové prostředky pouze k činnostem dané jeho pracovními povinnostmi nebo pracovní náplní. Je výslovně zakázáno používat autorizované počítačové prostředky pro osobní, podnikatelské nebo komerční účely. Je výslovně také zakázáno používat autorizované počítačové prostředky k činnostem, které jsou v rozporu s právními předpisy.

9. Služby poskytované uživateli

1. Výpočetní čas na autorizovaných počítačových prostředcích, včetně přístupu k aplikacím zakoupeným k obecnému využití v IS SML.
2. Uživatelskou a technickou podporu autorizovaných počítačových prostředků pořízených k obecnému využití v IS SML.
3. Přístup do veřejného internetu.
4. Správu a inovaci autorizovaných počítačových prostředků včetně učeben.
5. Zřizování a rušení přístupových účtů uživateli, jejich správu a údržbu.
6. Zálohování a archivaci všech dat uložených na serverech IS SML.
7. Zajištění komplexní správy elektronických certifikátů Postsignum (např. kvalifikované QCA, komerční VCA certifikáty, systémové certifikáty, apod.) v celém svém životním cyklu (žádost, instalace, prodloužení platnosti, ukončení platnosti, apod.). SML je oprávněno vydávat elektronické certifikáty Postsignum vlastními zdroji (oddělení informatiky a řízení procesů).

10. Vzdálený přístup do IS SML

1. V oprávněných případech je uživateli umožněn vzdálený přístup do IS SML NEVEŘEJNÝ. Vzdálený přístup je realizován vždy a pouze prostřednictvím zabezpečeného (šifrovaného) komunikačního kanálu VPN.
2. Vzdálený přístup do IS SML NEVEŘEJNÝ vždy podléhá schválení správci IS.
3. Uživateli je povoleno využívat vzdáleného přístupu do IS SML NEVEŘEJNÝ pouze z autorizovaných počítačových prostředků.

4. Vzdáleným přístupem lze z IS SML NEVEŘEJNÝ využívat jen následující služby:
   a) Elektronická poštovní schránka (e-mail).
   b) Veřejná část aplikace Konsiliář (https://podklady.liberec.cz/jednani/).
   c) Cloudové uložiště (https://cloud.liberec.cz/).
   d) Videokonference (https://vconf.liberec.cz/).

11. Povinnosti uživatele

1. Uživatel nesmí instalovat ani odinstalovat v rámci autorizovaných počítačových prostředků jakýkoliv SW včetně doplňků do webových prohlížečů i HW bez vědomí administrátora IS.
2. Je zakázáno kopírovat a distribuovat části operačního systému a nainstalovaného SW. SW je možné používat jen na takovou činnost, na kterou jsou určen.
3. Uživateli není dovolena neautorizovaná modifikace programů, dat nebo technického vybavení počítačů patřící pod IS SML. Zvlášť přísně jsou pak zakázány neautorizované změny počítačových prostředků, které by mohly mít vliv na provoz celé počítačové sítě.
4. Uživateli je zakázáno šířit a vědomě používat SW získaný v rozporu s právními předpisy, zejména autorským zákonem a smlouvou, kterou autor SW udělil svolení k jeho užití.
5. Každý uživatel je zodpovědný za zabezpečení počítačových prostředků proti zneužití (bezpečnostním incidentům).
6. Přístupová práva uživatele jsou dána jeho uživatelskou identifikací (přihlašovací jméno, heslo, případně další atributy sloužící k identifikaci uživatele) a členstvím ve skupinách. Uživatel se nesmí žádnými prostředky pokusit získat přístupová práva nebo privilegovaný stav, který mu nebyl přidělen administrátorem IS. Pokud uživatel získá privilegovaný stav nebo jemu nepříslušející přístupová práva jakýmkoli způsobem (včetně SW i HW chyby IS SML), je povinen tuto skutečnost neprodleně ohlásit administrátorovi IS. Toto se vztahuje na všechny počítačové prostředky. Uživatel se nesmí pokusit získat přístup k datům jiného uživatele. Uživatel je dále povinen v rámci svých uživatelských práv maximálně zabezpečit svoje data proti zneužití neoprávněnou osobou.
7. Uživatel je oprávněn pracovat na autorizovaných počítačových prostředcích pouze pod uživatelským jménem jemu přiděleným. 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.
8. Uživatel nesmí provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i v případech, kdy tento uživatel svá vlastní data explicitně nechrání.

9. 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.
10. Uživateli je zakázáno používat stejná (totožná) hesla v rámci IS SML a jeho soukromých aktivit (např. sociální sítě, elektronická pošta, e-shopy, banking, apod.).
11. 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) Heslo nesmí být nikdy prázdné.
    b) Nepoužívat uživatelské jméno, ani jeho přesmyčky nebo parafráze.
    c) Nepoužívat žádná data související s osobou uživatele (např. rodné číslo nebo jména uživatele, manžela (manželky), přítele (přítelkyně), dětí, psa, apod.).
    d) Nepoužívat v heslech znaky s diakritikou.
    e) Používat hesla o délce minimálně 8 znaků s výjimkou informačních systémů, které toto neumožňují.
    f) Používat hesla, která budou obsahovat malé písmeno, velké písmeno, jednu číslici a jeden speciální znak (např. /, -, _, $, &, apod.) s výjimkou informačních systémů, které toto neumožňují. Heslo musí vždy obsahovat minimálně kombinaci tří z výše uvedených kategorií znaků s výjimkou informačních systémů, které toto neumožňují.
    g) Měnit heslo minimálně jednou za 6 měsíců.
    h) Používat taková hesla, která si uživatel zapamatuje. Pro zapamatování hesel je doporučováno využívat mnemotechnické pomůcky.
12. Pro ochranu svých přihlašovacích údajů je uživatel povinen:
    a) Nesdělovat svá hesla jiné osobě, ani svým nadřízeným.
    b) Je výslovně zakázáno si hesla poznamenávat v listinné nezabezpečené formě (např. heslo napsané na zadní straně stolního kalendáře, nalepené heslo na klávesnici či monitoru, volný papírek s napsaným heslem uložený v šuplíku pracovního stolu, apod.) nebo v libovolné elektronické nezabezpečené formě (např. excel uložený na pracovní ploše počítače, na nezabezpečeném flashdisku, či v interní paměti telefonu, apod.).
    c) Okamžitě se odhlásit se z IS SML vždy, když nemůže zajistit nezneužití počítačových prostředků neoprávněnou 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 IS SML (bezpečnostní incident), provede bezodkladně všechny potřebné úkony pro změnu hesla.

13. V případě, že uživatel pro komunikaci s IS SML (např. e-mailový klient, kalendář, kontakty, uživatelská data, aplikace, apod.) využívá mobilních zařízení je povinen mít toto zařízení vždy zabezpečeno proti přístupu neoprávněnou osobou (např. otisk prstu, obraz obličeje, kódový zámek, apod.).
14. Uživatel plně zodpovídá za škody vzniklé zneužitím jeho přístupového oprávnění (loginu a hesla) k počítačovým prostředkům IS SML.
15. Pokud uživatel nemůže z jakýchkoliv důvodů pracovat po dobu delší než tři měsíce na počítačích, kde má uživatelské jméno (např. z důvodu služební cesty, dlouhodobé nemoci, apod.), sdělí tuto skutečnost prostřednictvím HelpDesku administrátorovi IS.
16. Bez svolení administrátora IS není uživatel oprávněn přemísťovat autorizované počítačové prostředky a odpojovat kabely. Toto omezení neplatí pro mobilní zařízení (např. notebooky, dataprojektory, tablety, mobilní telefony, apod.).
17. Bez svolení a asistence technika společnosti Kasro není uživatel oprávněn přemisťovat zařízení společnosti Kasro (tj. tiskárny a multifunkční reprografické zařízení).
18. Uživatel nesmí jakýmkoliv způsobem zasahovat do IS SML, kromě výměny spotřebního materiálu u tiskových a multifunkčních reprografických zařízení (tzn. papíru, papírových kotoučů, barvící pásky, toneru nebo inkoustu, apod.).
19. Úklid či jakékoliv jiné práce v místnostech vyčleněných výhradně pro počítačové prostředky (např. technologické centrum v budově nové Radnice, technologické centrum v budově Uran, technologická místnost v 1. patře budovy Radnice, technologická místnost v Liebiegově vile, apod.) je možno provádět pouze se svolením správce IS a za přítomnosti administrátora IS.
20. Uživateli je zakázáno jakkoliv manipulovat s aktivními či pasivními síťovými prvky IS SML.
21. Do zásuvek speciálního silnoproudého rozvodu je zakázáno zapojovat jiné spotřebiče než prvky počítačových prostředků.
22. Uživateli je zakázáno manipulovat s rozvodem elektrické energie a s kabeláží počítačových prostředků kromě osob k tomu určených.
23. Napájení některých počítačů je zálohováno bateriovým zdrojem elektrické energie UPS. K UPS je zakázáno připojovat jiná zařízení než vlastní počítač, tiskárnu, modem a zařízení IS SML.
24. Uživatel nesmí měnit mapování a sdílení disků vytvořených administrátorem IS.
25. Uživatel je povinen řídit se pokyny administrátora IS a dodržovat pracovní návody k provozu počítačových prostředků (směrnice, nařízení, pracovní postupy, uživatelské a administrátorské příručky, apod.).
26. Uživatel je povinen pracovat s autorizovanými počítačovými prostředky tak, aby je nepoškodil, zejména mechanicky (např. použití nepřiměřeně vysoké fyzické síly při ovládání počítačových prostředků, čištění počítačových prostředků chemickými

látkami způsobující jejich poškození, umístění počítačových prostředků na místech možného pádu z výšky, apod.).

27. Uživateli je zakázáno rozebírání autorizovaných počítačových prostředků včetně odstraňování krytu.
28. Uživatel je povinen chránit autorizované počítačové prostředky před jejich poškozením (např. umístění v dosahu přímého slunečního či jiného tepelného záření, umístění pod květináči – poškození z důvodu polití tekutinou, práce v podmínkách neslučitelných s provozními parametry počítačového prostředku, apod.).
29. Uživatel autorizovaných mobilních zařízení a notebooků je povinen tyto prostředky chránit před jejich zcizením či neoprávněnou manipulací (např. neponechávat počítačový prostředek v autě bez přítomnosti uživatele, půjčovat počítačový prostředek neoprávněné osobě, apod.).
30. Při přerušení práce se ztrátou dohledu nad počítačem (i při krátkodobém opuštění pracoviště) je uživatel povinen dostatečným způsobem zabránit neoprávněnému použití autorizovaných počítačových prostředků:
    a) Uzamknutím počítače – současným stiskem kláves „Windows“ + „L“.
    b) Uzamknutím počítače – současným stiskem kláves „Ctrl“ + „Alt“ + „Delete“ s následným výběrem volby Uzamknout počítač.
    c) Standardním ukončením práce s počítačem – vypnutím počítače.
31. V případě potřeby přístupu k datům nepřítomného uživatele jiným uživatelem zadá vedoucí příslušného odboru požadavek na HelpDesk s kopií výslovného písemného souhlasem daného nepřítomného uživatele k této operaci. V případě neexistence výslovného písemného souhlasu daného nepřítomného uživatele je postupováno vždy dle rozhodnutí tajemníka MML.
32. V počítačové síti je nainstalován antivirový program, který zabezpečuje antivirovou kontrolu souborů počítačů, počítačové sítě a elektronické pošty, včetně jejich příloh. Program vytváří na každém autorizovaném počítači rezidentní štít, který brání vniknutí a šíření škodlivého kódu do počítače. Antivirová databáze je prostřednictvím IS SML 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.
33. Pokud uživatel zjistí nebo je přímo účastníkem bezpečnostního incidentu (např. napadení počítače škodlivým kódem; ztráta nebo zcizení počítačových prostředků nebo dat; porušení práv subjektu údajů; únik osobních údajů, přístup neoprávněné osoby; apod.), je povinen okamžitě přerušit práci na počítačových prostředcích a neprodleně prokazatelným způsobem (např. HelpDesk, e-mail, interní sdělení, apod.) informovat administrátora IS a správce IS o bezpečnostním incidentu. Současně je uživatel o bezpečnostním incidentu HelpDesk informovat neprodleně telefonicky.

34. Uživatel je povinen veškeré nestandardní stavy IS SML, jím zjištěné, neprodleně hlásit prostřednictvím HelpDesku administrátorovi IS.
35. V blízkosti autorizovaných počítačových prostředků 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.
36. Uživatel je povinen dbát na řádné vypnutí počítačových prostředků po skončení práce (při odchodu domů), pokud není vyžadován nepřetržitý provoz těchto počítačových prostředků.
37. Uživatel je povinen při plnění svých pracovních povinností a úkolů vždy využívat ISZR v souladu s právními předpisy.
38. Uživatel je povinen zajistit administrátorům IS (popř. pracovníkům subdodavatele v doprovodu administrátora IS) přístup k autorizovaným počítačovým prostředkům, na kterých je prováděna jejich údržba nebo správa.
39. V případě potřeby uživatele předávat třetí straně větší množství dat, data větších velikostí či využívat k předání formu cloudových uložišť je uživatel povinen vždy používat zabezpečené cloudové uložiště. Pro tyto potřeby je v prostředí IS SML zřízeno vlastní cloudové úložiště – https://cloud.liberec.cz. Uživatele je zakázáno, zvláště pak v případech, kdy jsou obsahem předání dat či dokumentů osobní údaje, využívat cloudová úložiště typů např. Dropbox, Ulož.to, OneDrive, Google Drive, apod.

12. Ochrana osobních údajů

1. Uživatel je povinen plně dodržovat právní předpisy v souvislosti s ochranou osobních údajů fyzických osob, zvláště pak ustanovení nařízení Evropského parlamentu a Rady (EU) 2016/679 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) a zákona č. 110/2019 Sb. o zpracování osobních údajů, vše v platném znění.
2. V případě, že uživatel zjistí nebo je přímo účastníkem bezpečnostního incidentu porušení ochrany osobních údajů, je povinen okamžitě přerušit práci na počítačových prostředcích a neprodleně prokazatelným způsobem (např. HelpDesk, e-mail, interní sdělení, apod.) informovat tajemníka MML, pověřence pro ochranu osobních údajů (DPO), organizační oddělení tajemníka MML a správce IS o nastalém bezpečnostním incidentu. Podmínky, pravidla, procesní postupy ochrany osobních údajů jsou definována směrnicí rady města č. 17 RM Ochrana osobních údajů statutárního města Liberec.
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, datová schránka, zabezpečené úložiště dat (https://cloud.liberec.cz), přílohy opatřené heslem, šifrovaný flashdisk, apod.

4. Data obsahující osobní údaje mohou být uživatelem ukládána (platí i pro zálohy a archivaci dat) pouze v:
   a) Zabezpečených aplikací IS SML (např. spisová služba, ekonomický systém, stavební řízení, agenda přestupků, apod.).
   b) Datovém úložišti IS SML – sítové disky – složky adresářové struktury SML.
   c) Lokálním úložišti notebooků, které mají na příslušném disku zapnuto šifrování – lokální disk notebooku. Současně musí být notebook vždy chráněn přístupovým heslem.
   d) Externích paměťových médií, která mají zapnuto šifrování či jsou jinak zabezpečena proti možnému zneužití neoprávněnou osobou (např. dokument je opatřen heslem, apod.).
   e) Cloudovém úložišti dat IS SML (https://cloud.liberec.cz).
5. Uživateli je výslovně zakázáno pořizování kopií vedených osobních údajů libovolnou formou nad rámec jeho pracovní náplně a povinností (např. papírové kopie, pořizování fotografií či videí, ruční opisování, instalací speciálního SW k pořizování kopií obrazovky počítače, apod.).
6. Uživatel je povinen při ochraně osobních údajů brát na zřetel oblast sociálního inženýrství (Cílená manipulace osob za účelem provedení určité akce k získání určité informace nebo dat, např. neveřejná data organizace, osobní údaje, získání přístupu do IS SML, apod.).
7. Povinností uživatele předávajícího osobní údaje je vždy ověřit totožnost a oprávněnost osoby, která osobní data přebírá.
8. V případě zveřejnění dokumentů obsahujících osobní údaje je uživatel povinen tyto osobní údaje anonymizovat. Pro potřeby anonymizace osobních údajů elektronických dokumentů je v prostředí IS SML možnost využít aplikaci Signer.
9. Uživatel, který využívá pro přístup do své elektronické poštovní schránky veřejný internet, nese plnou odpovědnost za zabezpečení ochrany osobních údajů své poštovní schránce.

13. Povinnosti administrátora IS

1. Je povinen chránit data uživatelů a nakládat s nimi tak, aby nedošlo k jejich odhalení nebo zneužití. Dále nesmí tato data poskytovat třetí osobě bez výslovného svolení správce IS nebo tajemníka MML.
2. Nesmí mimo činnosti dané pracovní náplní administrátora IS prohlížet obsah dat nebo kopírovat jakákoliv data z autorizovaných počítačových prostředků bez výslovného svolení jejich vlastníka (uživatele) nebo správce IS nebo tajemníka MML.
3. Včas informovat uživatele o výpadcích IS SML.

14. Pravidla komunikace v počítačové síti

1. Uživateli je zakázáno využívat počítačové prostředky (především elektronické pošty) k obtěžování nebo zastrašování jiných uživatelů. Dále je zakázáno používat počítačových prostředků pro šíření obchodních dat, 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 uživatele.
2. Uživateli je zakázáno zneužívat autorizovaných počítačových prostředků k reklamním a jiným účelům, sloužícím k získání osobního prospěchu.
3. Uživateli je zakázáno používat autorizované počítačové prostředky k činnostem namířeným proti jakékoliv další organizaci, jejíž počítačové prostředky jsou dostupné prostřednictvím IS SML.
4. Uživatel je povinen dodržovat pravidlo, 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 s administrátorem IS a řídit se jeho pokyny.
5. Uživatel není oprávněn využívat nedovoleným způsobem autorizované počítačové prostředky, neoprávněně zkoušet, zkoumat nebo testovat jejich zranitelnost.
6. Uživatel při komunikaci v IS SML vždy dodržuje zásady slušného chování a obecně platných standardů v oblasti etikety. V případě, že uživatel komunikuje s administrátorem IS v rozporu s těmito zásadami a obecně platnými standardy slušného chování, může administrátor IS odmítnout uživateli poskytnout požadovanou službu (pomoc).

15. Bezpečnostní incident

1. Bezpečnostní incident je situace, při které došlo k ohrožení počítačových prostředků či k porušení definovaných pravidel. Bezpečnostní incident vzniká v důsledku selhání nebo nedodržení bezpečnostních opatření nebo porušení bezpečnostní politiky. Při bezpečnostním incidentu může dojít k ohrožení, ztrátě, odcizení, zneužití nebo změně počítačových prostředků.
2. Jako bezpečnostní incident se považuje i pouhý neúspěšný pokus, kdy došlo k ohrožení bezpečnosti počítačových prostředků či k porušení definovaných pravidel.
3. V případě nastalého bezpečnostního incidentu je administrátor IS nebo správce IS oprávněn okamžitě odpojit uživatele od počítačových prostředků.
4. Napadení počítače nebo serveru škodlivým kódem (různé formy počítačových virů) zapříčiněné svévolným počínáním uživatele v rozporu s ustanoveními této směrnice, resp. nedbalostí, je považováno porušení pracovní kázně zvlášť závažného charakteru.
5. Bezpečnostní incidenty jsou členěny podle závažnosti negativního vlivu na IS SML a podle velikosti rizika spojeného s jeho dalším provozem:

a) 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.

b) Bezpečnostní incidenty vysoké závažnosti – jsou takové stavy počítačových prostředků, které mění funkčnost systému a významným způsobem ovlivňují nebo omezují práci uživatele, např. nefunkčnost jednotlivých aplikací, zneužití počítačových prostředků neoprávněnou osobou, napadení počítače škodlivým kódem, apod.

c) Kritické bezpečnostní incidenty – jsou takové stavy počítačových prostředků, které brání provozu IS SML, např. dlouhodobé plošné výpadky veřejného internetu, dlouhodobé výpadky databázových nebo aplikačních serverů, ztráta konektivity k agendám provozovaných v rámci přenesené působnosti, ztráta nebo krádež počítačových prostředků obsahující osobní či neveřejné údaje, apod. V případě kritického bezpečnostního incidentu je vždy zpracován report o incidentu, který obsahuje minimálně popis incidentu, místo a čas vzniku incidentu, způsob komunikace, řešení a popis incidentu a definice preventivních opatření k zabránění opakování incidentu.

6. Příklady bezpečnostních incidentů (jako zvlášť významné bezpečnostní incidenty je nutné vnímat ty bezpečnostní incidenty, kdy data mající vztah k bezpečnostnímu incidentu obsahují osobní údaje):

a) Zcizení počítačových prostředků.

b) Ztráta počítačových prostředků.

c) Poškození počítačových prostředků.

d) Nález počítačových prostředků.

e) Vloupání do kanceláře.

f) Neoprávněný přístup k počítačovým prostředkům.

g) Neoprávněné použití počítačových prostředků.

h) Smazání dat.

i) Selhání infrastruktury nebo připojení.

j) Selhání serveru, databáze nebo aplikace.

k) Hackerský útok, penetrace do IS SML.

l) Virový útok – škodlivý kód.

m) Útok ransomware.

n) Přírodní katastrofa.

o) Falšování webové stránky (spoofing).

p) Pokus o zcizení počítačových prostředků.

q) Zneužití práv jiného uživatele.

r) Ztráta hesla.

s) Porušení integrity dat.

t) Ztráta důvěrnosti dat.

u) Doručení více jak 5 e-mailů během 5 minut do poštovní schránky uživatele s informací o nedoručitelnosti jeho odeslaných e-mailů.

v) apod.

16. Elektronická poštovní schránka (e-mail)

1. Každý uživatel má zřízenu nejméně jednu jednoznačnou e-mailovou schránku (obvykle ve tvaru prijmeni.jmeno@magistrat.liberec.cz) a má možnost doručovat a přijímat e-mail z IS SML NEVEŘEJNÝ. Součástí poštovní schránky je také kalendář, seznam kontaktů a seznam úkolů.
2. Poštovní schránka je standardně limitována velikostí 1,5 GB. Do velikosti poštovní schránky se počítá součet všech složek poštovní schránky včetně kalendáře, seznamu kontaktů a seznamu úkolů.
3. Případné navýšení velikosti poštovní schránky nad stanovený limit je možné pouze se svolením správce IS. Uživatel zadá požadavek na HelpDesk se zdůvodněním.
4. Pokud uživatel dosáhne 90 % kapacity velikosti poštovní schránky, je uživatel upozorněn automaticky každý den e-mailem o této skutečnosti.
5. Pokud uživatel dosáhne 100 % kapacity velikosti poštovní schránky (poštovní schránka je zaplněna), jsou přijaté e-maily poštovním serverem automaticky odmítnuty. Odesílatelům těchto e-mailů se budou hlásit jako nedoručitelné. Poštovní schránku je nutné vyčistit od nepotřebných poštovních zpráv.
6. Prostřednictvím e-mailové komunikace je zakázáno posílání osobních údajů s výjimkou případů, kdy je použito šifrované komunikace či využití jiného způsobu zabezpečení zasílaných osobních údajů.
7. Velikost přílohy (součet všech příloh) elektronické pošty nesmí přesáhnout 20 MB. Správce IS má právo systémově omezit velikost příloh.
8. V případě, že je uživateli do jeho poštovní schránky doručeno v jeden okamžik (v časovém rozmezí 5 minut) doručeno 5 a více e-mailových zpráv o nedoručitelnosti jeho odeslaných e-mailů, je uživatel povinen okamžitě kontaktovat administrátora IS.
9. Uživateli je umožněn přístup do své poštovní schránky také z veřejného internetu prostřednictvím webového rozhraní https://mail.liberec.cz nebo prostřednictvím komunikačních protokolů Exchange a Imap.
10. Uživateli je zakázáno používat elektronickou poštovní schránku pro účely soukromé komunikace včetně používání elektronické poštovní schránky k registracím (login) do

sociálních sítí, e-shopů, všech možných forem technických a uživatelských podpor, apod.

17. Diskové úložiště – síťové disky

1. Diskové úložiště je určeno k ukládání dat a dokumentů uživatele. Diskové úložiště je rozděleno do logických částí – síťových disků (např. disk T:, disk R:, apod.). Tyto logické síťové disky jsou dále pro přehlednost ukládaných dat a dokumentů členěny do adresářů (složek).
2. Na síťovém disku T: má každý uživatel standardně přidělenu kvótu 1 GB. Data uložená na disku T: jsou pravidelně (každou noc) zálohována.
3. Případné navýšení velikosti diskového úložiště na disku T: nad stanovený limit je možné pouze se svolením správce IS. Uživatel zadá požadavek na HelpDesk se zdůvodněním.
4. Po vyčerpání 90 % přidělené kapacity na disku T: je uživatel o této skutečnosti informován e-mailem.
5. Po vyčerpání 100 % přidělené kapacity na disku T: je uživateli odepřeno právo k zápisu. Ostatní operace (čtení a mazání) je uživateli umožněno.
6. Na síťovém disku R: má každý uživatel standardně přidělenu neomezenou velikost diskového prostoru. Disk R: slouží pouze jako archivní uložiště – archiv dokumentů. Na tomto disku není možné uživatelem mazat nebo provádět jiné úpravy. Pokud uživatel požaduje data uložit na disk R:, zadá požadavek na HelpDesk. Následně uživatel za součinnosti administrátora IS provede přesun dat na disk R:.

18. Uchovávání dat a dokumentů

1. Uživatel uchovává svá data v adresářích (složkách) na síťových discích.
2. Uživatel uchovává svá data v aplikacích oficiálně instalovaných administrátorem IS a schválených správcem IS.
3. Lokální disky počítačů nejsou určeny pro ukládání dat a dokumentů.
4. V případě, že uživatel uchovává data na lokálních discích počítačů, interní paměti mobilních telefonů či na externích paměťových médiích, vždy plně odpovídá za jejich zabezpečení.
5. Data uchovávaná na lokálních discích počítačů, interní paměti mobilních telefonů či na externích paměťových médiích nejsou zálohována ani archivována. Za takto umístěná data nenese administrátor IS či správce IS žádnou odpovědnost.
6. V případě potřeby předávání obsáhlých dat třetí straně je uživatel povinen používat zabezpečené formy předání těchto dat jako je například: šifrovaný e-mail, datová schránka, zabezpečené úložiště dat (https://cloud.liberec.cz), přílohy opatřené heslem, šifrovaný flashdisk, apod.

19. Tiskové a reprografické služby

1. Tiskové a reprografické služby jsou zajišťovány externě společností KASRO. Požadavky týkající se tiskových a reprografických služeb uživatel zadává standardně prostřednictvím HelpDesku.
2. Tiskové služby jsou poskytovány prostřednictvím zabezpečené tiskové fronty, tyto zabezpečené tiskové fronty se automaticky instalují pomocí doménové politiky správy IS SML.
3. Všechny tiskové fronty s výjimkou „Zabezpečený tisk COLOR“ jsou nastaveny pouze pro možnost tisku v černobílém režimu, a to včetně přímých tiskových front.
4. Uživatel má povinnost primárně používat černobílý tisk a kopírování. Používat služby barevného tisku a kopií je uživateli dovolenou pouze v opodstatněných případech.
5. Přímý tisk na multifukčním zařízení s instalovanou čtečkou čipových karet lze povolit jen ve výjimečných případech a vždy s povolením správce IS. Tento požadavek je vždy zadán na HelpDesk vedoucím příslušného odboru s odůvodněním.
6. U tiskáren a multifunkčních zařízení, které nemají instalovánu čtečku (terminály) čipových karet, se využívají přímé tiskové fronty. Tisk je možno provádět na této tiskárně nebo multifunkčním zařízení přímo, bez nutnosti používat čipové karty.
7. Tiskové a reprografické služby jsou zajišťovány a řízeny systémem SafeQ. Každá tisková úloha je předána serveru SafeQ. Ten pak tuto úlohu předá multifunkčnímu zařízení tam, kde je zrovna požadována. Úloha je zaúčtována na vrub uživatele nebo skupiny (oddělení, odbor). Úlohu lze vytisknout na jakémkoli multifunkčním zařízení (funkce follow-me) a tisky mohou být spravovány přímo na terminálu (např. opakovaný tisk, mazání, uložení, oblíbené položky, apod.).
8. Pro skenování na multifunkčních zařízeních je povinnost v maximální míře používat volbu „CompactPDF“. Tato volba skenuje data do PDF v komprimované podobě – výsledná velikost PDF dokumentu je menší. Pro vytváření materiálů do RM a ZM je tato forma skenování „povinná“ s výjimkou případů, kdy vyšší velikost skenovaného dokumentu (rozlišení) je nezbytná pro zobrazení detailu skenovaný dat (např. mapa, fotografie, apod.)
9. Uživatel má ve svých osobních složkách na disku T: vytvořenu podsložku „Scan“. Do této podsložky jsou automaticky ukládána data vyskenovaná za pomoci multifukčního zařízení. Podmínkou je identifikace uživatele prostřednictvím čtečky čipové karty na multifunkčním zařízení.

20. Provoz, redakční rada webu města a ostatní webové služby

1. Webové stránky statutárního města Liberce – www.liberec.cz – jsou provozovány formou služby. Poskytovatel služby odpovídá za provozuschopnost a dostupnost SW a HW prostředí webových stránek, neodpovídá za obsah, strukturu a grafickou podobu dat, které jsou na webových stránkách ukládány a zveřejňovány.

2. Za obsah, strukturu a grafickou podobu webových stránek je zodpovědná „Redakční rada webu“. V případě potřeby může „Redakční rada webu“ umožnit určené osobě „přispěvateli“ přístup do redakčního systému webu města (uživateli, externí administrátor webu, apod.).
3. Příslušný „přispěvatel“ odpovídá za věcnou správnost příspěvku, aktualizaci stránek příslušného odboru MML a úplnost dat uvedených na těchto webových stránkách města.
4. Redakční rada webu je v plné odpovědnosti vedoucího odboru kanceláře primátora.
5. Redakční rada webu:
   a) Schvaluje příspěvky přispěvatelů (určených osob v rámci odborů MML).
   b) Stanoví uzávěrku pro podávání příspěvků.
   c) Stanovuje uzávěrku pro podávání příspěvků.
   d) Stanovuje a odpovídá za grafickou úpravu webových stránek města.
   e) Definuje a odpovídá za obsahovou část webových stránek města.
   f) Definuje a odpovídá za strukturu webových stránek města.
6. Používání ostatních webových služeb, webových aplikací v IS SML musí být vždy předem projednáno a schváleno správcem IS.
7. Všechny webové služby, webové aplikace IS SML dostupné z veřejného internetu jsou (musí být) provozovány v zabezpečeném režimu (https). Tato zabezpečená komunikace zajišťuje autentizaci, důvěrnost přenášených dat a zajišťuje jejich integritu.

21. Sociální sítě

1. Uživateli je zakázáno v rámci IS SML používat sociální sítě nebo jakýmkoliv jiným způsobem přispívat nebo využívat služeb sociálních sítí.
2. Uživateli je zakázáno v rámci sociálních sítí vytvářet (zakládat) uživatelské účty nebo profily jménem SML. Tato povinnost se vztahuje komplexně na činnosti pracovního i soukromého charakteru, na pracovní i mimopracovní dobu uživatele.
3. V případě, že uživatel k plnění svých pracovních povinností nezbytně potřebuje využívat služeb sociální sítě nebo založit na sociální síti účet či profil jménem SML, může tak učinit pouze na základě tajemníkem MML schváleného požadavku, zadaného vedoucím příslušného odboru na HelpDesk. V případě uvolněného člena zastupitelstva města Liberec není vyžadována podmínka schválení tajemníkem MML.

22. Pořízení a implementace nového SW do IS SML NEVEŘEJNÝ

1. Do IS SML NEVEŘEJNÝ může být pořízen a implementován pouze SW schválený správcem IS.

2. SW musí být vždy plně kompatibilní s provozovaným operačním systémem autorizovaných počítačů – MS Windows v aktuální verzi.
3. SW musí splňovat standardy informačního systému veřejné správy.
4. SW musí umožnovat chránit přístup uživatelským účtem s jednoznačným heslem. Heslo musí umožňovat, aby jej mohl uživatel změnit. Heslo musí umožnovat nastavit jeho platnost a vyžadovat potřebnou komplexnost (velké písmeno, malé písmeno, speciální znak a číslo) včetně délky hesla.
5. Všechny činnosti SW včetně zásahů administrátora musí být zaznamenány ve formě log souborů. Tyto log souboru se musí umět centrálně sbírat nástroji k tomu určenými.
6. Pokud je SW přístupný přes tenkého klienta z internetu, musí SW umožňovat tuto komunikaci šifrovat certifikátem (HTTPS).
7. SW musí umět členit uživatelské účty do různých rolí.
8. SW musí mít schopnost uživatelské účty napojit na centrální správu uživatelských účtů v active direktory.
9. Pokud SW v rámci svého datového modelu obsahuje veřejně dostupné údaje, musí SW obsahovat rozhraní, které umožní tyto údaje přečíst z externího zdroje ve strojově čitelné formě bez požadavku na dodavatele (autora) systému.

23. Klíčový uživatel

1. Hlavním úkolem klíčového uživatele je jeho aktivní účast při řešení požadavků na danou aplikaci a jeho případný rozvoj. Ve své podstatě je klíčový uživatel garantem dané aplikace za stranu SML.
2. Definice klíčového uživatele:
   a) Je komunikačním a metodickým partnerem administrátora IS při řešení požadavků provozního i rozvojového charakteru.
   b) Má přehled o základních vlastnostech a funkcionalitách dané aplikace. Jeho znalosti o dané aplikaci přesahují rámec běžného uživatele.
   c) Koordinuje a zajišťuje činnosti spojené s řešením provozních i rozvojových požadavků na straně SML – organizační opatření, testování nových funkcí aplikace, kontrola dat, apod.
   d) Aktivně se podílí na rozvoji aplikace (je členem řešitelského týmu). Toto zahrnuje i rozvojové aktivity směrem k integracím s ostatními aplikacemi IS SML.
   e) Podílí se na testování nových verzí dané aplikace. Spolurozhoduje o nasazení nové verze do produktivního provozu.
   f) Vytváří nebo se podílí na vytváření metodických standardů práce s danou aplikací.
   g) V případě protichůdných požadavků navrhuje a spolurozhoduje o směru řešení daného požadavku.

h) Podílí se na sestavování plánu o obsahu školení uživatelů.

i) Informuje svého nadřízeného případně tajemníka MML o aktuálním stavu dané aplikace.

j) V případě havárie aplikace nebo ztráty dat se podílí na činnostech spojených s obnovou aplikace nebo dat do provozuschopného stavu na straně SML.

k) Je informován o výpadcích, plánovaných údržbách nebo změnách nastavení dané aplikace.

l) Je odpovědný za správu, údržbu a plnění uživatelských číselníků dané aplikace.

m) V rámci možností (tam, kde to aplikace umožňuje) provádí uživatelské nastavení aplikace.

3. Klíčového uživatele pro danou konkrétní aplikaci určuje vedoucí příslušného odboru nebo tajemník MML.

4. Seznam aplikací s určením garanta (odboru) klíčového uživatele

a) Odbor ekonomiky:

- Ekonomický systém – Ginis.
- Pohledávkový systém – Proxio.

b) Stavební úřad:

- Stavební řízení – Vita Software.

c) Odbor vnitřních věcí:

- Spisová služba – eSpis.
- Elektronická řídící kontrola – Croseus.
- Registr smluv – Ginis.
- Podklady pro RM a ZM – Konsiliář.
- Docházka – PowerKey.
- Mzdový systém – FluxPam.
- Vyvolávací systém – Tetronik.
- Tiskové a kopírovací služby – Kasro.
- Hlasové služby – VoIP.

d) Tajemník:

- Podněty, stížnosti, petice – Proxio.

e) Kancelář primátora:

- Redakční systém včetně webových stránek – WebJet.

f) Odbor školství a sociálních věcí:

- Domovní evidenční systém – iDES.
- Elektronické zápisy do ZŠ a MŠ – RedWeb.
- Správa fondů – Grantys.

g) Odbor územního plánování:

- GIS, geostore V6, passporty.

h) Odbor správní a živnostenský:

- Volební agenda – CityWare.
- Agendy přenesené působnosti vykonávané odborem.

i) Odbor dopravy:

- Přestupky – Vita Software.
- Agendy přenesené působnosti vykonávané odborem.

j) Odbor právní a veřejných zakázek:

- Veřejné zakázky – eZak.
- Právní systém – Codexis.

k) Odbor správy veřejného majetku:

- Evidence věcných břemen – Marushka.
- Hlášení podnětů – Marushka Photo.
- Vyjadřovací služba - Marushka.
- Evidence hřbitovní správy – MP Orga.

24. Uživatelská podpora (HelpDesk, požadavky, řešení havarijních stavů)

1. Uživatel předává veškeré své požadavky na uživatelskou podporu v oblasti IS SML prostřednictvím:
   a) Aplikace HelpDesk na adrese https://helpdesk.liberec.cz/.
   b) V případě nefunkčního počítače telefonicky na telefonním čísle (48524) 3555.
2. Pracovní doba uživatelské podpory je zajištěna v:
   a) Pondělí a středu: od 8:00 do 17:00 hodin.
   b) Úterý a čtvrtek: od 8:00 do 16:00 hodin.
   c) Pátek: od 8:00 hodin do 12:00 hodin.
   d) Sobota: není zajišťována.
3. Požadavek na přidělení nebo upgrade počítačových prostředků uživateli (s výjimkou uvolněných členů Zastupitelstva města Liberec), může zadat pouze vedoucí příslušného odboru nebo tajemník MML. Požadavek musí být vždy zadán na

HelpDesk, kde bude posouzen a schválen správcem IS. Tento typ požadavku bude vedoucím příslušného odboru či tajemníkem MML vždy zdůvodněn.

4. Požadavek na přidělení nebo upgrade počítačových prostředků uvolněnému členu Zastupitelstva města Liberec, může zadat pouze uvolněný člen Zastupitelstva města Liberec. Požadavek musí být vždy zadán na HelpDesk, kde bude posouzen a schválen správcem IS. Tento typ požadavku bude uvolněným členem Zastupitelstva města Liberec vždy zdůvodněn.
5. V případě požadavku na přidělení nebo upgrade počítačových prostředků (např. větší monitor, ergonomická myš, apod.) ze zdravotních důvodů, musí být nedílnou součástí požadavku zadaného na HelpDesk vyjádření závodního lékaře.
6. Požadavek na zřízení elektronického podpisu (tj. kvalifikovaný certifikát PostSignum QCA nebo komerční certifikát PostSignum VCA) pro uživatele zadá prostřednictvím HelpDesku vedoucí příslušného odboru. Součástí žádosti (požadavku) jsou údaje o uživateli, pro kterého má být certifikát vydán (jméno a příjmení, popř. titul) a zdůvodnění (účel použití certifikátu).
7. V rámci aplikace HelpDesk má uživatel možnost ohodnotit svoji spokojenost s řešením daného požadavku. V případě, že uživatel tuto možnost nevyužije a spokojenost s řešením požadavku není ohodnocena, bude aplikací HelpDesk automaticky přiřazeno neutrální hodnocení.

25. Přístupová práva a oprávnění

1. Ukládání dat – veškerá data jsou uložena v adresářích (složkách), která odpovídá organizačnímu schématu MML. Pro každý odbor MML je vytvořen adresář (složka) obsahující podadresáře (podsložky) pro jednotlivá oddělení. Pro každý odbor a oddělení je zřízen sdílený adresář. V kořenovém adresáři je zřízen sdílený adresář pro ukládání a sdílení dat a dokumentů mezi odbory.
2. Standardní nastavení přístupových oprávnění pro přístup složek adresářové struktury SML:
   a) Uvolnění členové Zastupitelstva města Liberec:
      - Kompletní přístup do složek určených pro uvolněné členy Zastupitelstva města Liberec. Přístupová práva jsou nastavována individuálně dle reálných a oprávněných potřeb uvolněného člena Zastupitelstva města Liberec.
      - Omezený přístup do sdílených složek v rámci SML. Přístupová práva jsou nastavována individuálně dle reálných a oprávněných potřeb.

   b) Tajemník MML a jeho zástupce:
      - Přístup pro čtení do všech složek odborů v adresářové struktuře SML.
      - Kompletní přístup do sdílených složek v rámci SML.

   c) Vedoucí odboru a jeho zástupce:
      - Přístup pro čtení do všech složek v adresářové struktuře odboru.

- Kompletní přístup do sdílených složek v rámci odboru a oddělení.
- Omezený přístup do sdílených složek v rámci SML. Přístupová práva jsou nastavována individuálně dle reálných a oprávněných potřeb.

d) Vedoucí oddělení a jeho zástupce:

- Přístup pro čtení do všech složek v adresářové struktuře oddělení.
- Kompletní přístup do sdílené složky v rámci oddělení.
- Omezený přístup do sdílených složek v rámci odboru a SML. Přístupová práva jsou nastavována individuálně dle reálných a oprávněných potřeb.

e) Ostatní uživatelé

- Každému uživateli odboru je zřízena osobní složka. Uživatel má do této složky kompletní přístup.
- Omezený přístup do sdílených složek v rámci oddělení, odboru a SML. Přístupová práva jsou nastavována individuálně dle reálných a oprávněných potřeb.

3. Řešení speciálních požadavků na přístupová oprávnění do adresářové struktury SML:

a) Požadavek na speciální nastavení přístupových práv musí být se zdůvodněním zadán na HelpDesk. Tento typ požadavku může být na HelpDesk zadán pouze vedoucím příslušného odboru nebo tajemníkem MML. Pro uvolněné členy Zastupitelstva města Liberec může být tento typ požadavku zadán pouze tajemníkem MML.

b) O požadavku na nastavení speciálních přístupových práv rozhoduje:

- Do celé adresářové struktury IS SML vždy správce IS nebo tajemník MML. Tato podmínka platí i pro nastavení přístupových práv pro uvolněné členy Zastupitelstva města Liberec.
- Do adresářové struktury odboru vždy vedoucí příslušného odboru.

4. Interní přístupová práva aplikací:

a) Jedná se o aplikace, které jsou součástí IS SML a mají vlastní seznam přístupových oprávnění, který neodpovídá běžným uživatelským účtům.

b) Pro aplikaci je jmenován odpovědný administrátor IS přidělující přístupová oprávnění.

c) Požadavek na nastavení přístupových práv uživatele do aplikací musí být se zdůvodněním zadán na HelpDesk. Tento typ požadavku může být na HelpDesk zadán pouze vedoucím příslušného odboru nebo tajemníkem MML. Pro uvolněné členy Zastupitelstva města Liberec může být tento typ požadavku zadán pouze tajemníkem MML.

5. V případě podezření na závažné porušení pracovních povinností uživatelem je možné v IS SML dohledat některé aktivity uživatele (např. e-mailová komunikace, historie

telefonních hovorů, čas přihlášení nebo odhlášení, apod.). Poskytnutí těchto dat (aktivit) třetí osobě může být ze strany administrátora IS provedeno pouze na základě prokazatelného svolení tajemníka MML. Veškeré takto poskytnutá data musí být vždy v souladu s právními předpisy.

26. Zálohování a archivace dat

1. Data uložená na síťových discích jsou zálohována pravidelně každý den v nočních hodinách. Data uložená na síťových discích jsou zálohována maximálně 30 kalendářních dnů zpětně.
2. Data uložená na síťových discích jsou archivována jednou ročně (obvykle listopad).
3. E-mailové schránky jsou zálohovány pravidelně každý den v nočních hodinách. E-mailové schránky jsou zálohovány maximálně 30 kalendářních dnů zpětně.
4. Data uložená v aplikacích jsou zálohována pravidelně každý den v nočních hodinách.

27. Zahájení pracovního vztahu uživatele, přesun na jinou pracovní pozici

1. Personální oddělení MML při zahájení pracovní vztahu uživatele nebo přesunu uživatele na jinou pracovní pozici (dále jen zahájení pracovního vztahu uživatele) v dostatečném časovém předstihu (dle reálných možností daného konkrétního zahájení či přesunu), zpravidla 5 pracovních dnů předem, zadá na HelpDesk požadavek na zahájení úkonů spojených se zahájením pracovního vztahu.
2. Vedoucí příslušného odboru definuje rozsah počítačových prostředků nového uživatele.
3. Uživatel nastupující do hlavního pracovního poměru (jeho pozice je definována v organizačním řádu MML) má nárok na plné vybavení počítačovými prostředky. Uživateli jsou přiděleny vždy jen takové počítačové prostředky, které jsou nezbytné pro plnění jeho pracovních povinností daných jeho pracovní náplní.
4. Uživatel nastupující do jiného než hlavního pracovního poměru (činnosti vykonávané v rámci odborné praxe či stáže, dohoda o provedení práce, dohoda o pracovní činnosti, apod. – jeho pozice není definována v organizačním řádu MML) nemá standardně nárok na vybavení počítačovými prostředky. Uživateli jsou v oprávněných případech přiděleny jen omezené počítačové prostředky, a to v rozsahu počítače bez možnosti přímého přístupu k aplikacím a datům IS SML a elektronické poštovní schránky. Výjimku nad toto pravidlo může udělit pouze tajemník MML a to zadáním požadavku na HelpDesk s popisem požadovaných počítačových prostředků včetně zdůvodnění této výjimky.

28. Ukončení pracovního vztahu uživatele

1. Personální oddělení MML při ukončení pracovního vztahu (jedná se o všechny formy pracovního vztahu) uživatele v dostatečném časovém předstihu (dle reálných možností daného konkrétního ukončení pracovního vztahu), zpravidla 5 pracovních dnů předem, zadá na HelpDesk požadavek na zahájení úkonů spojených s ukončením pracovního

vztahu uživatele. Nedílnou součástí požadavku bude uvedení data (datum), ke kterému pracovní vztah uživatele končí.

2. Administrátor IS nejpozději ke dni ukončení pracovního vztahu zajistí zneplatnění všech přístupových práv ke všem počítačovým prostředkům uživatele.
3. Nejpozději ke dni ukončení pracovního vztahu je uživatel povinen předat administrátorovi IS veškeré mu svěřené počítačové prostředky.
4. Nejpozději ke dni ukončení pracovního vztahu je uživatel povinen předat administrátorovi IS svůj osobní pracovní adresář umístěný na síťovém disku zcela prázdný. Pokud takto neučiní a v jeho osobním pracovním adresáři zůstanou data, budou následně administrátorem IS po 14 dnech od ukončení pracovního vztahu tato data překopírována do osobní složky vedoucího příslušného odboru na disk R:.
5. Nejpozději ke dni ukončení pracovního vztahu je uživatel povinen kompletně vyčistit svoji osobní elektronickou poštovní schránku (e-mail). Pokud takto neučiní a v jeho osobní poštovní schránce zůstanou data, budou následně administrátorem IS po 14 dnech od ukončení pracovního vztahu tato data nenávratně smazána bez jejich archivace.
6. Nejpozději ke dni ukončení pracovního vztahu je uživatel povinen předat administrátorovi IS svůj cloud (https://cloud.liberec.cz) zcela prázdný. Pokud takto neučiní a v jeho cloudu zůstanou data, budou následně administrátorem IS po 14 dnech od ukončení pracovního vztahu tato data nenávratně smazána bez jejich archivace.
7. Nejpozději ke dni ukončení pracovního vztahu je uživatel povinen předat veškerou svoji pracovní elektronickou agendu (např. spisová služba, ekonomický systém, stavební řízení, přestupkové řízení, pohledávkový systém, apod., data uložená ve společných složkách/adresářích, apod.) svému nástupci nebo jinému uživateli určeného vedoucím příslušného odboru. Pokud takto uživatel neučiní, budou administrátorem IS data vedená v aplikacích IS SML po 14 dnech od ukončení pracovního vztahu tato data převedena na vedoucího příslušného odboru.
8. Nejpozději ke dni ukončení pracovního vztahu je uživatel povinen zajistit zneplatnění kvalifikovaného (QCA) případně komerčního (VCA) certifikátu, pokud uživatel vlastní token i jeho vrácení. Kontaktní osobou pro úkony spojené se zneplatněním certifikátů a vrácením tokenu je administrátorem IS (VVOI).
9. U uživatele, který končí pracovní vztah (jedná se o všechny formy pracovního vztahu), odpovídá vedoucí příslušného odboru za předání veškeré elektronické agendy (např. e-mailová komunikace, spisová služba, ekonomický systém, ostatní data aplikací, data umístěná v osobních i společných složkách/adresářích, apod.) jeho nástupci nebo jím určenému uživateli. Tuto svoji odpovědnost (povinnost) vedoucí příslušného odboru vždy stvrzuje svým podpisem na „Výstupním listu“ uživatele.
10. Bez splnění výše uvedených povinností při ukončení pracovního vztahu nebude uživateli ze strany administrátora IS potvrzen „Výstupní list“.

29. Export dat z informačního systému evidence obyvatel (ISEO)

1. Export dat z informačního systému evidence obyvatel (ISEO) a jejich následné úkony s nimi jsou v plné odpovědnosti vedoucího příslušného odboru, který o tyto data žádá.
2. S daty z informačního systému evidence obyvatel má určený uživatel povinnost nakládat vždy v souladu s právními předpisy, zvláště pak z pohledu možného vzniku bezpečnostního incidentu.

30. Porušení směrnice a sankce

1. Administrátor IS nebo správce IS má právo zrušit (ukončit) přístup k počítačovým prostředkům uživateli, který prokazatelně porušil ustanovení této směrnice, a to na dobu potřebnou k novému definování přístupových práv vedoucím příslušného odboru daného uživatele. Toto právo se vztahuje i na případy vzniku bezpečnostního incidentu.
2. V případě porušení této směrnice mohou být vůči uživateli uplatněny sankce podle obecně závazných právních předpisů, případně jiných interních předpisů SML.
3. V případě vzniku škod na IS SML se postupuje v souladu s interními předpisy SML.

31. Požadované základní dovednosti uživatele

1. Všichni uživatelé jsou povinni ovládat počítačové prostředky IS SML, potřebné pro výkon jejich pracovní náplně nebo pracovních povinností a v rámci uživateli přidělené pracovní pozice.
2. Základní funkce a aplikace:
   a) Operační systém Microsoft Windows.
   b) Microsoft WORD.
   c) Microsoft EXCEL.
   d) Microsoft POWERPOINT
   e) Microsoft Explorer.
   f) Firefox Browser.
   g) Google Chrome.
   h) Spisová služba.
   i) Aplikace potřebné pro výkon pracovní pozice např. GINIS, eSpis, Croseus, Marushka, Proxio, VITA SW, Konsiliář, apod.
   j) Práce s certifikáty.
3. V rámci přijímacího řízení je zpravidla u nového potencionálního uživatele ověřena úroveň počítačových dovedností.

32. Závěrečná ustanovení

1. Tato směrnice nahrazuje směrnici tajemníka 12T Provoz IS MML.
2. Směrnice nabývá účinnosti 1. 7. 2020.

Seznam změn a revizí řízeného dokumentu

Verze	Datum vydání /revize/	Č. usnesení rady města	Účinnost	Popis změny / revize	Zpracovatel
1.	1. 7. 2020	XXX	1. 7. 2020	Vydání směrnice	Ing. Zbyněk Vavřina