Jihomoravský kraj Krajský úřad Jihomoravského kraje Žerotínovo nám. 3/5 Brno	Interní normativní akt KrÚ směrnice **PROVOZ HW A SW**	Evidenční číslo	
		11/INA-KrÚ	
		Číslo vydání:	5
		Účinnost od:	25.11.2011

Pravidla používání výpočetní techniky, počítačové sítě a užívání software

OBSAH:

ZPRACOVAL:	OVĚŘIL:	SCHVÁLIL:	ZÁVAZNÝ PRO:
OI	OI	JUDr. Věra Vojáčková ředitelka KrÚ	KrÚ
Ing. Jan Forbelský	Ing. Jan Forbelský		
Datum a podpis: 15.11.2011 Ing. Jan Forbelský, v.r.	Datum a podpis: 15.11.2011 Ing. Jan Forbelský, v.r.	Datum a podpis: 16.11.2011 JUDr. Věra Vojáčková, v.r.	

1 ÚVOD

1.1 Předmět a účel

Účelem této směrnice je stanovení pravidel pro provozování výpočetní techniky, lokální počítačové sítě JMK, Internetu, elektronické pošty, informačních systémů v rámci KrÚ.
Cílem tohoto dokumentu je zajistit provozování výpočetní techniky, lokální počítačové sítě, Internetu, elektronické pošty a informačních systémů výlučně oprávněnými uživateli, zamezit možnosti neoprávněného získání a zneužití dat a zvláště osobních údajů a zajistit důsledný soulad provozování informačních systémů s platnými právními předpisy.

1.2 Použité zkratky

AD	Active Directory (systém adresářových služeb firmy Microsoft)
BIOS	program uložený na základní desce počítače (Basic Input Output System)
DDHM	drobný dlouhodobý hmotný majetek
DHM	dlouhodobý hmotný majetek
DMS	Správce dokumentů JMK
e-mail	elektronická pošta (electronic mail)
HW	hardware
ISVS	informační systém veřejné správy
LAN	lokální počítačová síť (Local Area Network)
NB	notebook
ODHS	odd. hospodářské správy
ODORG	odd. organizační
OMA	Outlook Mobile Access - podoba pro mobilní zařízení PDA, SmartPhone, Palm,..
OPVV	odd. personálních věcí a vzdělávání
OWA	Outlook Web Access – webový přístup k el. poště
PC	počítač (osobní počítač, Personal Computer)
SW	software
VPN	virtuální privátní síť – slouží k propojení vzdálených míst úřadu
VT	výpočetní technika
WWW	World Wide Web – celosvětová počítačová síť Internet

1.3 Vymezení základních pojmů

Lokálně uložená data
Data uložená lokálně na diskovém prostoru PC, NB nebo přenosném médiu nemohou být centrálně zálohována a za jejich bezpečnost plně odpovídá uživatel.

Centrálně uložená data
Data ukládaná centrálně jsou uložena na datových úložištích, kde jsou technicky zabezpečena proti ztrátě a pravidelně zálohována. Přístup k nim je specifikován pro každého uživatele zvlášť.

Informační systém
Informační systém je soubor lidí, technologických prostředků a metod, které zabezpečují sběr, přenos, zpracování a uchování dat za účelem tvorby prezentace informací pro potřeby uživatelů. Příkladem informačního systému může být kartotéka, telefonní seznam, kniha došlé pošty nebo účetnictví. Systém nemusí být nutně automatizovaný pomocí počítačů a může být i v papírové podobě.

Informacemi míníme sdělení, které odstraňuje nejistotu nebo nevědomost, daty míníme jakékoli zaznamenané poznatky či fakta. Jako zvláštní pojem zde vystupuje také znalost představující zobecnění poznání určité části reality. Informaci je možno také chápat jako data s nějakým přidaným významem (data + význam). Informace je údaj (množné číslo data), ke kterým si člověk přiřadí význam.

Správce sítě
Zaměstnanec OI, pověřený správou LAN.

Správce SW
Správce SW je pracovník OI, pověřený správou a evidencí SW v úřadu.

Uživatel
Každý zaměstnanec, stážista, člen ZJMK, pracovník vykonávající práci na základě dohody o pracovní činnosti či dohody o provedení práce, poradci využívající PC, LAN a informační systém jako nástroj k plnění pracovních povinností.

Uživatelský účet
Množina uživatelských práv definovaná pro uživatele v prostředí LAN, která jednoznačně definuje uživatele a jeho pracovní prostředí.

Pracovník technického servisu
Pracovník externí firmy provádějící servis na základě uzavřené smlouvy nebo vystavené objednávky v rozsahu této smlouvy nebo objednávky.

Software
SW (též programové vybavení) je v informatice sada všech počítačových programů používaných v PC, které provádějí nějakou činnost. SW lze rozdělit na systémový SW, který zajišťuje chod samotného PC a jeho styk s okolím a na aplikační SW, se kterým buď pracuje uživatel PC nebo zajišťuje řízení nějakého stroje.

V souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, je počítačový program, pokud splňuje znaky autorského díla, chráněn zákonem (jak vyplývá i z dalších mezinárodních úmluv o autorských právech). Autorský zákon chrání všechny aspekty nakládání s počítačovým programem, mj. práva držitele autorských práv k počítačovému programu, a zaručuje držiteli autorských práv řadu exkluzivních práv, zejména pak právo na integritu díla a právo na jeho šíření.

Evidenční list výpočetní techniky
Seznam, ve kterém je specifikována konfigurace a lokalizace PC, který užívá uživatel. Jedná se o seznam v elektronické podobě, který lze aktuálně generovat z aplikace HelpDesk.

1.4 Související dokumentace

- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů,
- zákon č. 106/ 1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, (dále jen „zákon č. 106/1999 Sb.“)

- zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, (dále jen „Zákoník práce“)
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění zákona č. 190/2009 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, ve znění pozdějších předpisů,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů,
- zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů,
- nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů,
- vyhláška č. 496/2004 Sb., o elektronických podatelnách,
- vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby,
- vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů,
- vyhláška č. 194/2009 Sb., o stanovení podrobností užívání informačního systému datových schránek,
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací,

- *3/INA-KrÚ Spisový řád*
- *4/INA KrÚ Podpisový řád*
- *9/INA KrÚ Řízení dokumentace*
- *34/INA KrÚ Příručka kvality*

2 VÝPOČETNÍ TECHNIKA

2.1 Evidence výpočetní techniky

V rámci platných právních norem a dokumentů KrÚ provádí základní evidenci zařízení VT OKŘ. VT jsou přidělena inventární čísla DDHM, resp. DHM. Rozšířenou evidenci zařízení VT včetně příslušenství vede ve specializovaném programu HelpDesk OI. Rozsah a logiku rozšířené evidence určuje vedoucí OI v závislosti na vnitřní logice programu, v němž je evidence vedena.

2.2 Základní pravidla práce s výpočetní technikou

Prostředky VT (HW a SW) se na KrÚ používají pouze **pro plnění pracovních povinností** a po dobu nezbytně nutnou (viz Zákoník práce, § 301 písm. b). „Zaměstnanci jsou povinni využívat pracovní dobu a výrobní prostředky k vykonávání svěřených prací, plnit kvalitně a včas pracovní úkoly.“ nebo § 316 odst. 1: „Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně VT ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.“

Zaměstnavatel ke kontrole využití VT používá SW, kterým lze zjistit jaké programy a na jak dlouhou dobu uživatel na svém PC spouští.

Zařízení VT se zapíná a vypíná síťovým vypínačem nebo spínačem. Postup vypnutí počítače je uveden níže. Nikdy se nezapíná nebo nevypíná zasunutím vidlice přívodního kabelu do napájecí zásuvky.

Při vypínání prostředků VT je třeba dodržet následující podmínky:
PC se vždy vypíná až po regulérním ukončení všech spuštěných aplikací, nikdy při otevřené nebo běžící aplikaci. Výjimku tvoří uvedení PC do „režimu spánku“, které lze provést i při spuštěných aplikacích a lze jím nahradit vypnutí PC při dočasném opuštění pracoviště. Pokud použitý operační systém umožňuje vypínání PC, zásadně při vypínání počítačů používáme prostředky operačního systému. Vypínání PC vypínačem (popř. jeho resetování tlačítkem Reset) používáme jen ve výjimečných případech, kdy PC nelze vypnout prostředky operačního systému nebo kdy operační systém vypínání PC neumožňuje. Periferní zařízení zapínáme a vypínáme síťovým vypínačem, je zakázáno vypínat zařízení VT odpojením vidlice přívodního kabelu z napájecí zásuvky. Mezi vypnutím a opětovným zapnutím VT musí být ponechána časová prodleva minimálně 5 sekund. Laserovou tiskárnu není dovoleno vypnout v průběhu tisku. Je-li třeba zrušit tisk, je možno ze zásobníku papíru odebrat zásobu papíru, počkat na dotištění posledního listu papíru a po jeho dotištění tiskárnu vypnout.

Uživatelé mají možnost tiskových výstupů na tiskárny přidělované podle potřeb vyplývajících z funkce uživatele a provozních možností. Uživateli nevzniká automaticky nárok na přidělení vlastní tiskárny. Z důvodu efektivního využívání techniky jsou tiskárny sdíleny více uživateli. Pokud je sdílená tiskárna připojena k pracovní stanici, není nutné pro zpřístupnění tisku přihlášení uživatele (stačí PC pouze zapnout). Tiskárny, které jsou vybaveny vlastním síťovým adaptérem (jsou připojeny přímo do sítě), jsou přístupné kdykoliv. Z důvodu vyšší hospodárnosti v maximální možné míře (pokud to tiskárna a povaha dokumentu umožňuje) nastavit při tisku „oboustranný tisk (duplex)“ a omezit barevné tisky. Spotřební materiál k tiskárnám (tonery a inkousty) si uživatelé mohou vyměnit na OI vždy výměnou za prázdný kus (náplně jsou většinou renovovány).

Na PC je možno používat pouze SW instalovaný OI.

Osobě, která není v zaměstnaneckém poměru k úřadu, popř. v poměru vyplývajícím ze zastávané funkce, je přístup k VT používané v úřadu přísně zakázán s výjimkami stanovenými touto směrnicí. K jakémukoliv PC mají kromě oprávněných uživatelů odboru, na němž je PC umístěn, kdykoliv povolen přístup také ŘKrÚ nebo její zástupce, pracovník OI, pracovník technického servisu s povolením pracovníka OI, zaměstnanec jiného odboru KrÚ výhradně s povolením VO, na němž je PC nainstalován, jiná osoba výhradně s povolením ŘKrÚ (resp. jejím zástupcem) nebo vedoucího OI (resp. jeho zástupce).

Všichni uživatelé prostředků VT jsou povinni dodržovat základní technické a provozní podmínky používání VT dle této INA tak, aby nedošlo k poškození VT, dodržovat při práci takové podmínky, aby nemohlo dojít k odcizení prostředků VT, odcizení a zneužití dat, zejména dat obsahujících osobní údaje a důvěrné informace o KrÚ, prozrazení, odcizení a neoprávněnému použití jakýchkoliv hesel, přístupových kódů a jiných SW a HW prostředků sloužících k autentifikaci oprávněného uživatele. Při přerušení práce jsou uživatelé povinni uvést prostředky VT do takového stavu, aby nemohlo dojít k jejich zneužití nepovolanou osobou. Při krátkodobém odchodu od PC - uzamknout PC (stiskem klávesy s logem Windows + L, nebo CTRL + Alt + Del a výběrem požadovaného úkonu). Při předpokladu delší

nepřítomnosti (nad 30 min.) - odhlásit se od systému (stiskem kláves CTRL + Alt + Del a výběrem požadovaného úkonu nebo přes nabídku Start), zachovávat mlčenlivost o všech bezpečnostních opatřeních přijatých k zabezpečení prostředků VT, LAN a dat. Je nutné se podrobně seznamovat s pokyny pracovníků OI pro používání VT a tyto pokyny dodržovat.

Uživatelům PC je zakázáno:

- Provádět jakýkoliv zásah do zařízení VT včetně jejího přemisťování, jakkoliv manipulovat s datovými kabely LAN, samostatně připojovat (resp. odpojovat) PC do LAN (resp. z LAN). Výjimku tvoří NB a mobilní technika.
- Samostatně připojovat PC do prostředí Internetu nebo do jakéhokoliv vnějšího prostředí (jak prostřednictvím LAN, tak jakýmkoliv jiným způsobem – např. pomocí modemu), výjimku tvoří NB a mobilní technika.
- Povolit přístup k VT nebo zásah do VT jiným osobám než osobám stanoveným v této směrnici, provádět systémové úpravy a změny HW a SW, samostatně povolovat sdílení prostředků PC (sdílení disků, složek, tiskáren atd.), při práci s PC jíst, pít a kouřit, uchovávat na pracovišti jiné datové nosiče než datové nosiče používané pro služební účely. Datové nosiče používané pro služební účely jsou takové datové nosiče, které byly uživatelem získány v rámci KrÚ za účelem plnění pracovních povinností a obsahující pouze data nezbytná pro plnění pracovních povinností (zejména diskety, CD, DVD, flash disky).
- Vkládat do PC jiné datové nosiče než datové nosiče používané pro služební účely a určené OI k zálohování dat nebo k užívání legálně nainstalovaného SW.
- Instalovat do PC jakýkoliv SW, ponechávat zařízení VT zapnuté a bez dozoru po skončení pracovní doby. Výjimka je instalace antivirů. Všechny zde nezmíněné způsoby nakládání s VT musí být v souladu s platnými právními normami a interními předpisy KrÚ.
- Nastavovat BIOS PC (jsou oprávněni pouze pracovníci OI).

Uživatelům je dovoleno používat služby počítačové sítě v pracovní dny od 6.00 do 20.00 hodin. Mimo tuto dobu není provoz sítě plně garantován - může být prováděna profylaxe systému a pravidelné zálohování dat. Jednorázové požadavky na práci v počítačové síti v době od 20.00 do 6.00 hodin a v nepracovních dnech povoluje správce sítě na základě souhlasu vedoucího OI.

2.3 Používání mobilní výpočetní techniky

Mobilní výpočetní technikou jsou NB, laptopy, chytré telefony, tablet PC a obdobné prostředky VT včetně periferních zařízení a příslušenství. Mobilní VT se používá pouze pro plnění pracovních povinností. Oprávnění uživatelé mobilní VT mají právo mobilní VT včetně periferních zařízení a příslušenství používat jak v prostorách KrÚ, tak i mimo prostory KrÚ.

Oprávněným uživatelem mobilní VT může být VO, pracovník odboru, na nějž byla VT přidělena s povolením VO, ŘKrÚ, člen samosprávy nebo uživatel, jemuž byla mobilní technika svěřena na základě písemného předávacího protokolu do stálého užívání nebo krátkodobý uživatel, který o krátkodobou zápůjčku požádá prostřednictvím HelpDesku. Předání techniky potvrdí v zápůjční knize.

Oprávněný uživatel mobilní VT je povinen zabezpečit používanou mobilní VT a data na ní uložená proti odcizení a zneužití. Oprávněný uživatel je povinen zejména neponechávat mobilní VT v neuzamčených prostorech nebo bez dohledu, v automobilech (ani v uzamčených), používat dostupné formy mechanického a elektronického zabezpečení mobilní VT a dat na ní uložených (mechanické zabezpečení bránící odcizení, použití hesla pro

přístup do mobilní VT apod.). Při jakémkoliv vzdálení se od spuštěného PC (NB), je uživatel povinen tento uzamknout (stisknutím kombinace kláves Windows + L, nebo CTRL + Alt + Del a výběrem požadovaného úkonu). Při předpokladu delší nepřítomnosti (nad 30 min.) - odhlásit se od systému.

Vzdálené připojení ke zdrojům úřadu, ať pomocí OWA, nebo VPN, může být aktivní jen po nezbytně nutnou dobu a nesmí být zpřístupněno neoprávněné osobě. Pokud tomu nebrání zvláštní okolnosti (nemoc či jiná dlouhodobá nepřítomnost na pracovišti) minimálně jednou za 14 kalendářních dnů musí být NB fyzicky připojen kabelem do počítačové sítě v budovách KrÚ z důvodu aktualizací SW, instalací opravných záplat a aktualizaci antivirového programu. Při nedodržení této lhůty může být správcem zablokován účet daného NB v doméně.

Pracovníci OI jsou oprávněni v případě, že nebude k dispozici dostatečně výkonná mobilní VT, použít při plnění pracovních povinností mimo prostory KrÚ i standardní VT včetně periferních zařízení a příslušenství. Povolení k takovému použití VT je oprávněn dát vedoucí OI, ŘKrÚ nebo její pověřený zástupce.

3 POČÍTAČOVÁ SÍŤ

3.1 Pravidla pro práci v lokální počítačové síti

Počítačová síť KrÚ je provozována na platformě Microsoft 2003 Server a její provoz je řízen doménovými řadiči. Doména má název „kr-jihomoravsky“. Každý uživatel prostředků LANmusí mít vytvořen uživatelský účet. Termínem uživatelský účet v LAN je zde myšlen účet v adresářové službě Active Directory (AD). Tvar uživatelského účtu je popsán v článku 3.2.
Uživatelské účty v LAN zřizuje, mění a ruší správce sítě na základě vyplnění údajů OPVV v aplikaci Sharepoint webové části **„Pracovní poměr – jen pro oprávněné osoby“,** bude obsahovat jméno a příjmení pracovníka, osobní číslo a číslo pracovního místa. Lokalizaci pracoviště (budova, podlaží, číslo kanceláře, telefon) zadá ODHS. Seznam požadovaných oprávnění v rámci LAN bude zadáno VO prostřednictvím systému HelpDesk. Uživateli budou přidělena jen práva nezbytně nutná pro plnění jeho pracovních povinností. Pokud VO bude pro pracovníka požadovat přidělení práv, která pro výkon jeho pracovních povinností nejsou nezbytně nutná, je správce sítě oprávněn tato práva nepřidělit. Správce sítě zřídí uživatelský účet tak, aby při prvním přihlášení byl uživatel vyzván k zadání hesla. Přístupové heslo sestavuje, zadává a mění uživatel dle pokynů obsažených v těchto pravidlech článku 3.3. Uživatel nese plnou zodpovědnost za prozrazení (tím je myšleno i sdělení hesla jinému pracovníkovi úřadu), odcizení, ztrátu a zneužití hesla. Nadřízený pracovník nesmí požadovat po uživateli sdělení hesla k jeho uživatelskému účtu. V případě nepřítomnosti uživatele musí být přijata taková organizační opatření, aby nebylo nutné přihlášení nepřítomného uživatele (např. přesměrování pošty na kolegu apod.). VO je povinen v případě, že pracovník odboru přestane vykonávat činnosti, ke kterým měl dříve definována v rámci LAN oprávnění, neprodleně požádat správce sítě o zrušení těchto oprávnění pro daného pracovníka. OPVV nahlásí neprodleně do aplikace Sharepoint webové části **„Pracovní poměr – jen pro oprávněné osoby“,** že pracovník, který měl zřízen účet v LAN, ukončil pracovní poměr u KrÚ, ukončil práci na odboru a pracuje na jiném odboru KrÚ, odešel na mateřskou či rodičovskou dovolenou. VO nahlásí neprodleně do aplikace HelpDesk, že pracovník, který měl zřízen účet v LAN, z jakéhokoliv důvodu dále nebude trvale nebo dočasně používat svůj účet v LAN (např. pracovní neschopnost). Ve výše uvedených případech musí být účet

neprodleně zrušen nebo zablokován (ve výjimečných případech je možno na žádost VO na dobu 1 měsíce účet ponechat, je ale nutno okamžitě změnit heslo).
První pracovní den následující po dni ukončení pracovního poměru nebo odchodu na mateřskou dovolenou vypálí OI obsah složky Dokumenty na medium a oproti podpisu předá VO příslušného odboru nebo jeho asistentce/sekretářce. Podle potřeb lze vypálit i poštovní soubor pst. Nevyzvednutá media budou po uplynutí 3 měsíců od vypálení skartována.

3.2 Uživatelské jméno (účet)

Tvar uživatelského jména je: **prijmeni.jmeno** (výjimku tvoří univerzální konta, používaná více pracovníky), kde **„prijmeni“** je příjmením uživatele a **„jmeno“** je křestní jméno uživatele. U jmen příliš dlouhých, je křestní jméno zkráceno a při shodě jmen, je řešeno individuálně.

3.3 Heslo

K uživatelskému jménu přináleží heslo. Prvotní (dočasné) heslo při zřízení účtu stanoví administrátor a je nutno ho při prvním použití změnit.

Konvence pro zadávání hesla:
Minimální délka hesla je 6 znaků. Heslo musí být kombinací velkých písmen, malých písmen a musí obsahovat alespoň jeden speciální znak nebo číslici. Heslo nesmí obsahovat část uživatelského jména a diakritiku. Platnost hesla je 182 dnů.
Příklad správně utvořeného hesla: kx7V#Pp.
Za správný tvar hesla je zodpovědný uživatel, který má oprávnění toto heslo zadávat a měnit. Heslo lze změnit kdykoliv po zadání kombinace kláves Ctrl+Alt+Del a výběru možnosti Změnit heslo. Heslo musí být psáno vždy tak, jak bylo uloženo, to znamená, že záleží na velikosti písmen a použití (nepoužití) znamének diakritiky. Heslo přináleží kontu uživatele a **nesmí** být sdělováno jiným uživatelům. Za jeho zneužití odpovídá uživatel. Doménová politika je nastavena tak, že třetí chybně zadané heslo uzamkne uživatelský účet na 1hod. Účet může před vypršením tohoto intervalu odemknout administrátor na žádost uživatele. V případě, že uživatel své heslo zapomene, požádá administrátora o jeho změnu. Administrátor v takovém případě nahradí stávající heslo uživatele dočasným, které sdělí uživateli. Toto heslo je jednorázové a při prvním použití je nutno ho změnit. Administrátor může zpřístupnit uživatelské konto jinému uživateli pouze na základě písemné žádosti vedoucího dotčeného odboru (např. při dlouhodobé nemoci, dovolené apod.). Některé aplikace, které nejsou propojeny s adresářovou službou domény, vyžadují zadávání zvláštních uživatelských jmen a hesel. Tato uživatelská jména a hesla nepodléhají výše uvedeným konvencím a jejich režim je řešen individuálně.

3.4 Složka Dokumenty

Běžně zpracovávaná data je uživatel povinen ukládat do složky **Dokumenty,** která je směrována na uživatelovu složku v centrálním úložišti dat. Data, která uživatel bude sdílet s jinými uživateli, např. v rámci odboru, nebo oddělení, je uživatel povinen ukládat na mapovaný disk O (Odbory). Pokud uživatel uloží svá data do jiné složky na svém disku nebo na plochu, tedy lokálně, nese plnou odpovědnost za jejich ztrátu v případě poruchy pevného disku PC. Složka Dokumenty **nesmí být použita pro ukládání dat nesouvisejících s pracovní náplní,** např. hudby, soukromých obrázků, fotografií, apod.

3.5 Centrální úložiště

Centrální úložiště je v síti krajského úřadu provozováno na diskovém poli souborového serveru. Na tomto úložišti se ukládají data jednotlivých uživatelů v jejich osobních složkách, kam je přesměrovaná i jejich složka Dokumenty. Dále se z něj uživatelům „mapují“ (= vzdáleně připojují) síťový disk O: a případně další disky, vyžadované některými aplikacemi.

Složka Dokumenty
Uživatel má výhradní přístup ke svým datům, ve své uživatelské složce, kam je přesměrována složka Dokumenty v profilu uživatele a je nastaven offline přístup k této složce vč. synchronizace. Znamená to, že uživatel pracuje s dokumenty na serveru a v případě výpadku sítě pracuje s lokální offline kopií daného dokumentu. Po obnovení provozu sítě se provede automatická synchronizace dokumentů. Na tomto disku je nastavena tzv. disková kvóta = povolený objem ukládaných dat.

Mapovaný disk O (Odbory)
Dále má uživatel přístup ke sdílené složce odboru. Tato složka je přístupná pouze pracovníkům daného odboru a slouží především k ukládání sdílených dat tohoto odboru. Automaticky je zřízen přístup všech pracovníků k adresáři odboru. Na požádání VO může být vytvořen i adresář pro oddělení a přístup do něj pro danou skupinu uživatelů.

Výměna
Součástí disku O: je i složka Výměna, do které mají všichni uživatelé plný přístup (tedy možnost vkládat i odstraňovat data). Složka Výměna slouží k předávání zejména objemných dat v rámci úřadu. Uživatel, který si z této složky stáhne data pro něj určená, je povinen tato data ze složky odstranit. Složka Výměna slouží jako dočasné úložiště a data v ní uložená jsou **pravidelně jednou týdně administrátorem odstraněna.**

Uchovávání většího objemu dat - archivace
Uživatelé, kteří mají potřebu uchovávat větší objemy dat, zejména takových, ke kterým nepřistupují příliš často, mohou požádat o jejich vypálení na CD-ROM nebo DVD-ROM některého ze spolupracovníků nebo pracovníka OI a jejich kopii mohou ukládat lokálně na svých PC.

3.6 Přemístění techniky

Uživatel nesmí bez vědomí OI přemísťovat VT s výjimku NB a mobilní techniky (viz bod 2.2). V případě potřeby přestěhování techniky požádá o toto uživatel OI prostřednictvím aplikace HelpDesk. Plánované přesuny pracovníků i s VT (změna dislokace kanceláří), podléhají rovněž schválení OI. Ponechání VT na odboru při ukončení pracovního poměru uživatele povoluje VO a podléhá schválení OI (posuzuje se zejména technická stránka). V opačném případě OI danou VT odveze k dalšímu využití a provede změnu v aplikaci HelpDesk.

3.7 Hlášení závad a přidělování techniky

Závady na VT je povinen uživatel neprodleně hlásit na odd. uživatelské podpory OI prostřednictvím aplikace HelpDesk příp. telefonicky na linku 1414. Průběh řešení požadavku zadavatel může sledovat v aplikaci HelpDesk. V případě vyřešení požadavku jiným způsobem nebo jeho neaktuálnosti je zadavatel povinen ohlásit toto na OI. Uživatel má právo na OI hlásit připomínky a nedostatky, podávat návrhy a podněty související s provozem serverů nebo s provozem uživatelských programů prostřednictvím aplikace HelpDesk. Pracovní

stanice jsou uživatelům přidělovány na základě potřeby, vyplývající z jejich funkce, provozních potřeb a technických možností (např. způsobu připojení do sítě). Při změně funkce nevzniká uživateli automaticky nárok na doposud používané prostředky VT.

3.8 Fyzické zabezpečení výpočetní techniky

Místnosti, v nichž je umístěna VT (zejména PC obsahující data s osobními údaji) a místnosti, v nichž jsou uloženy datové nosiče se zálohami dat, je nutno v rozumné míře zabezpečit proti úmyslnému i neúmyslnému poškození a proti odcizení VT a datových nosičů. Místnosti, kde jsou umístěny servery a uloženy zálohy dat serverů, musí být kromě prvků pasivní bezpečnosti zabezpečeny také prvky aktivní bezpečnosti – elektronickou požární signalizací a elektronickou zabezpečovací signalizací. Místnosti kde, jsou umístěny aktivní prvky LAN, musí být kromě prvků pasivní bezpečnosti zabezpečeny také elektronickou požární signalizací, pokud to umožňují rozvody této slaboproudé sítě. Nutnost instalace elektronické zabezpečovací signalizace bude posouzena pro každý jednotlivý případ zvlášť.

3.9 Antivirová ochrana

Antivirovým systémem musí být povinně vybaven každý PC, z něhož je přistupováno do prostředí Internetu, na němž je přijímána a odesílána elektronická pošta, z něhož je prováděna komunikace s osobami a objekty vně LAN KrÚ jiným způsobem než s využitím Internetu a elektronické pošty (např. komunikace pomocí modemu), na němž je instalován poštovní server, sloužící jako brána do Internetu. Antivirový program instaluje a konfiguruje odpovědný pracovník OI. Uživateli PC, na němž je nainstalován a nakonfigurován antivirový program, se přísně zakazuje jakkoliv měnit nastavení a konfiguraci antivirového programu, zejména vypínat rezidentní části antivirového programu a měnit naplánované automatické antivirové testy. Na NB je instalována antivirová ochrana včetně Firewallu. Update antivirových programů je pro PC připojené k počítačové síti prováděn automaticky. Na PC nepřipojených do počítačové sítě provádí update pověřený pracovník OI. Uživatel, který zjistí, že je jeho PC zavirován nebo že obdržel zavirovanou poštu, uvědomí o tomto faktu pracovníky OI. Aby nedocházelo ke zpomalení PC v pracovní době vlivem jejich testování na přítomnost virů, je antivirová kontrola prováděna vždy v noci ze středy na čtvrtek. Uživatelům proto doporučujeme ponechat ve středu při odchodu z práce PC zapnutý a uzamčený. Pokud tak neučiní, bude antivirová kontrola provedena automaticky při nejbližším zapnutí PC.

3.10 Zálohování dat

Data v adresáři Dokumenty jsou pravidelně zálohována. Tato problematika je řešena pracovním postupem na OI.

4 ELEKTRONICKÁ POŠTA A INTERNET

4.1 Pravidla používání elektronické pošty

KrÚ provozuje vlastní primární poštovní server Email. Zde je uložen obsah veškerých poštovních schránek, dále pak veřejné složky a globální adresář. Na poštovním serveru je instalován antivirový program, který provádí prvotní antivirovou kontrolu příchozí pošty. Elektronická pošta, která zůstane uložena na poštovním serveru je v pravidelných intervalech zálohována. K práci s elektronickou poštou na KrÚ je používán Microsoft Outlook a jeho webová podoba Outlook Web Access (OWA) a podoba pro mobilní zařízení Outlook Mobile Access (OMA). Schránku elektronické pošty zřizuje a adresu přiděluje pověřený pracovník OI na základě vyplnění údajů v aplikaci Sharepoint webové části **„Pracovní poměr – jen pro**

oprávněné osoby". Údaje vyplní pověřený pracovník OKŘ OPVV (údaje musí obsahovat minimálně následující informace: jméno a příjmení uživatele, odbor, oddělení a funkční zařazení uživatele). Vedoucí odboru, na který nový pracovník nastupuje, sdělí, ve které kanceláři a na kterém PC bude elektronická pošta přijímána a odesílána. Přístup do schránky je chráněn heslem. Formát adresy osobní poštovní schránky je **prijmeni.jmeno@kr-jihomoravsky.cz.** Je-li jméno uživatele příliš dlouhé, nebo existují-li dva uživatelé stejného příjemní a jména, bude formát adresy upraven pracovníkem OI. Kromě adresy má každá schránka ještě tzv. „zobrazované jméno", kterým se schránka zobrazuje v adresáři a rovněž v poli „Od" resp. „Komu" v poštovní zprávě. Formát zobrazovaného jména je: **Příjmení Jméno.** Kromě osobních schránek jednotlivých uživatelů jsou na serveru provozovány **schránky organizační** pro jednotlivé odbory a poštovní schránka podatelny. Organizační schránku obsluhuje zaměstnanec určený VO. VO doplní tuto povinnost do popisu pracovní činnosti zaměstnance a stanoví mu povinnost kontrolovat obsah schránky nejméně 2x denně. Poštovní schránka elektronické podatelny je obsluhována pověřeným zaměstnancem OKŘ. Povinností zaměstnance je kontrolovat schránku nejméně 2x denně, v 8 hod. a ve 13 hod. Postup zpracování elektronických podání stanoví směrnice č. *3/INA-KrÚ Spisový řád.*

Každý PC, na němž je možno přijímat a odesílat elektronickou poštu, musí být vybaven antivirovou ochranou. Tato antivirová ochrana umí kromě kontroly vlastního PC provádět také kontrolu příchozí a odchozí pošty (druhá kontrola příchozí pošty). Pokud nebudou volné licence antivirového systému, bude zřizování nových schránek pozastaveno do doby zajištění nových licencí.

Velikost zprávy, kterou poštovní server zpracuje, je stanovena na max. 10 MB. Limit pro hromadné odesílání objemných zpráv je stanoven na 20 MB celkového objemu – to znamená, že např. 10 adresátům lze najednou odeslat zprávu o velikosti max. 2 MB (10 * 2 MB = 20 MB). Za překročení limitu odpovídá odesílatel. Za velikost poštovní schránky odpovídá uživatel. **Velikost poštovní schránky uživatele je omezena** následujícími limity:

- varování uživatele při dosažení 80 % povolené kapacity,
- znemožnění odesílání zpráv při dosažení 90 % povolené kapacity,
- znemožnění příjmu zpráv při dosažení 100 % povolené kapacity.

Kapacitu povoluje pracovník OI a tato problematika je řešena pracovním postupem na OI.

Uživatelé elektronické pošty jsou povinni nezneužívat elektronickou poštu pro mimopracovní účely (viz Zákoník práce, § 301, písm. b) nebo § 316 odst. 1). Zaměstnavatel má právo a povinnost, kontrolovat, zda zaměstnanci nezneužívají jeho majetek k soukromým účelům a proto prověřuje, jak často a v jakém rozsahu zaměstnanci využívají elektronickou poštu pro soukromou potřebu.

Zaměstnavatel využívá ke kontrole veškeré elektronické pošty antispamový SW (GFiMailEssential). Zprávy vyhodnocené jako spam jsou podle nastavených kritérií zpracovány a dále buď odeslány uživateli, zařazeny do nevyžádané pošty nebo na dobu jednoho měsíce odloženy do určeného adresáře. Správci aplikace jsou zobrazeny hlavičky zpráv, tj. datum odeslání, odesilatel, adresát/i a předmět zprávy.

Při čtení elektronické pošty zachovávat maximální obezřetnost. Uživatelé nesmí otevírat e-mail, který je jakkoliv podezřelý, např. z následujících důvodů: je nevyžádaný a neočekávaný, zaslaný od neznámého nebo podezřelého odesilatele, je v jiném jazyce, než je očekáváno, nabízí přílohu s podezřelou tematikou, nesouvisející s pracovní náplní (erotika, hry, obrázky, tapety, spořiče apod.). Uživatel je povinen nejméně 2x denně zkontrolovat, zda nemá ve své osobní nebo sdílené schránce zprávu, v případě celodenní nepřítomnosti použít tzv. „Službu mimo kancelář" a v případě nutnosti pomocí „Průvodce pravidly..." nastavit přeposílání kopie zpráv na jiného pracovníka, případně mu jiným způsobem zpřístupnit svou

schránku (nastavením oprávnění), v případě obdržení pošty (stížnosti, petice, žádosti o poskytnutí informací podle zákona 106/1999 Sb., jiná úřední písemnost, apod.) do osobní poštovní schránky uživatele, je tento povinen postupovat v souladu s platnou směrnicí č. *3/INA-KrÚ Spisový řád.*

Uživatelům elektronické pošty je přísně zakázáno používat elektronickou poštu pro přenos dat obsahujících osobní údaje nebo důvěrné informace o úřadu mimo LAN KrÚ (tedy na jiné adresy než adresy v doméně kr-jihomoravsky.cz) bez povolení odpovědné osoby. Uživatelům je zakázáno rozesílat elektronickou poštou zprávy s jakoukoliv přílohou pomocí distribučního seznamu „všem z KrÚ JMK" – k tomu využít prostor na Intranetu KrÚ. Pracovník OI pověřený správou elektronické pošty je oprávněn konfigurovat systém tak, aby automaticky odfiltroval elektronickou poštu s jakýmikoliv přílohami, které mohou být potenciálně napadeny viry nebo s jejichž využitím se viry, červy a jiné formy nebezpečných programů šíří (např. spustitelné přílohy typu .com a .exe, přílohy typu .vbs, .bat, .pif apod.), jsou zavirované, zjevně neslouží k plnění pracovních povinností.

Filtrace elektronické pošty je prováděna v rozsahu stanoveném vedoucím OI, pokud to umožňují používané softwarové prostředky, zejména pak konfigurovat systém tak, aby automaticky odfiltroval elektronickou poštu obtěžující nebo nebezpečnou (SPAM apod.), ručně odstranit poštu zavirovanou, podezřelou, zjevně nesouvisející s plněním pracovních povinností, znepřístupnit poštovní schránku uživatele, který jedná v rozporu s těmito pravidly, provádět nastavení jakýchkoliv filtrů a omezení s cílem zamezit hrozbě útoku a průniku do LAN KrÚ (odfiltrování veškeré pošty z podezřelého zdroje apod.).

Vzhledem k tomu, že elektronická pošta úřadu není určena pro nepracovní účely, může úřad provádět **monitorování, přesměrování a ukládání veškeré příchozí i odchozí elektronické pošty.** Monitorování a ukládání elektronické pošty je prováděno automaticky v rozsahu umožněném použitými softwarovými prostředky. Přesměrování nebo sdílení elektronické pošty z jedné adresy na jinou adresu je možné na žádost uživatele adresy, která má být přesměrována nebo jeho přímého nadřízeného.

Pro archivaci elektronické pošty je nainstalován a zprovozněn program GFI MailArchiver. Podle nastavených pravidel je archivována pošta příchozí, odchozí a interní, která je přístupna jen přihlášenému uživateli. Archivované zprávy je možné vyhledat podle zadaných kritérií a tyto pak vytisknout, uložit nebo obnovit.

Přístup uživatele z vně KrÚ k poštovní schránce je možný pomocí tzv. Outlook Web Accessu, z kteréhokoliv PC s přístupem k Internetu (doma, v internetové kavárně, v jiné organizaci). Tento přístup se provádí pomocí internetového prohlížeče, kde do pole „Adresa" uživatel napíše: https://email.kr-jihomoravsky.cz/exchange. Poté se uživatel přihlásí zadáním svého uživatelského jména a hesla (před něž ještě vloží název domény a obrácené lomítko – kr-jihomoravsky\uzivatelske.jmeno). Další možností vzdáleného přístupu k poště je Outlook Mobile Access (OMA), který umožňuje zabezpečený přístup k elektronické poště z mobilních zařízení.

4.2 Přístup k internetu

Připojení LAN do prostředí Internetu je zabezpečeno firewallem (zabezpečení počítačové sítě proti útokům z Internetu), na mobilních zařízeních tzv. personálním firewallem. Přístup uživatelů ke stránkám v Internetu je řízen proxy serverem, přístup je povolen pouze přihlášeným uživatelům. Pro řízení přístupů k Internetu je používán software Kernun Web

Filter. Provozní omezení vyplývající z tohoto způsobu zabezpečení (nepřístupnost některých služeb a režimů práce v prostředí Internetu) jsou nezbytná pro zajištění bezpečnosti LAN. Zabezpečovací funkce způsobující tato omezení nebudou ani krátkodobě deaktivovány.
Uživatelé Internetu jsou povinni:

- Internet používat výhradně k plnění pracovních povinností, zaměstnavatel ve smyslu § 316 zákoníku práce kontroluje, zda zaměstnanci nezneužívají jeho majetek k soukromým účelům a proto prověřuje, jak často a které internetové stránky zaměstnanci navštěvují. Kontrola navštívených stránek probíhá pomocí softwaru Kernun Web Filter, který zaznamenává stránky navštívené uživatelem. Tento SW umožňuje kategorizovat stránky a omezit popř. zakázat přístup na ně,
- vyvarovat se navštěvování podezřelých stránek, protože ty mohou být zdrojem nebezpečného virového útoku (stránky s erotickou tématikou, hackerské stránky apod.). Pokud budou na podezřelou stránku automaticky přesměrováni, musí takovou stránku neprodleně opustit.

Uživatelům Internetu s výjimkou pracovníků OI se zakazuje:

- měnit nastavení a konfiguraci připojení do Internetu,
- stahovat z Internetu jakýkoliv SW (včetně zdarma nabízeného SW). Je zakázáno stahování nejen komerčních produktů, ale i shareware (volně šiřitelné pro nekomerční účely), freeware (volně šiřitelné), cardware (volně šiřitelné po zaslání pohlednice), addware (pro přidání některých funkcí do windows), public domain software, ovladačů, spořičů obrazovky, wallpapers (tapet), plug-in, snap-in apod. (přídavných modulů), klientů přístupu k síťovým operačním systémům a adresářovým službám, trial (zkušebních) verzí SW, demonstračních verzí SW, počítačových her, oprav a úprav SW(upgradů, updatů, bezpečnostních updatů, aktualizací, oprav chyb) apod.,
- stahovat z Internetu multimediální obsah (hudba, video), a to včetně těch, které jsou nabízeny k volnému stažení. Pokud půjde o obsah potřebný k plnění pracovních povinností, zajistí stažení těchto dat pracovníci OI, pokud to dovolí velikost stahovaných dat a technické možnosti VT,
- instalovat a používat programy pro internetové telefonování, on-line diskuse a chatování.
- přijímat pomocí Internetu radiové a televizní vysílání (s výjimkou pracovníků OI a těch, u nichž to vyžaduje pracovní náplň),
- zúčastňovat se internetových videokonferencí, které nesouvisejí s pracovními povinnostmi
- přistupovat na stránky s erotickou tématikou a stahovat z Internetu jakékoliv materiály s erotickou tématikou,
- přistupovat na stránky s nezákonnou a nevhodnou tematikou (fašismus, terorismus, pedofilie, stránky hackerů apod.) a cokoliv z nich stahovat,
- pracovat s Internetem jakýmkoliv způsobem, který by porušoval platné zákony, právní úpravy a interní předpisy KrÚ.

Důvodem výše uvedených zákazů je zejména zajištění bezpečnosti LAN, dodržování právních norem a zajištění dostatečné propustnosti připojení do Internetu (omezená šíře pásma).

4.3 Internetové stránky KrÚ

KrÚ provozuje tyto typy internetových stránek:

- Webový portál JMK – oficiální veřejný portál JMK a KrÚ přístupný všem uživatelům Internetu (www.kr-jihomoravsky.cz)
- Intranet - interní portál přístupný pouze uživatelům s účtem v AD
- Extranet – portál přístupný z veřejné internetové sítě pouze po přihlášení (http://www.kr-jihomoravsky.cz/dms)

Webové stránky portálu systémově spravuje pověřený pracovník OI – správce webových stránek. Zajišťuje jejich vývoj, nasazení, funkčnost a přípravu grafických šablon. Udržuje redakční systém (RS) pro vkládání a administraci dat, správu uživatelů a jejich oprávnění podle rolí a struktury složek stejně jako školení odpovědných osob za publikování. Na intranetu v části Dokumenty – Publikační systém zveřejňuje a aktualizuje seznam osob zapojených do RS, postupy, návody, zásady, nápovědu a další informace pro publikování, kterými jsou odpovědné osoby povinny se řídit.
Pro každou složku (agendu) na portálu musí být stanoveny vedoucím odboru za danou složku tyto role – autor, redaktor, šéfredaktor.
Autor vytváří v dané složce nové dokumenty, které připravuje a formátuje podle zveřejněných postupů, návodů a zásad na intranetu. (Stav „Ke schválení“).
Redaktor schvaluje správnost obsahu, popisu a umístění dokumentů a zodpovídá za aktuálnost a úplnost dat v RS i na portálu. (Stav „Ke zveřejnění“).
Šéfredaktor zveřejňuje připravené dokumenty na portálu a kontroluje podobu zveřejněných dat včetně dalších sekcí - „Téma“, „Aktuality“. (Stav „Zveřejněný“).
Jednotlivé role lze slučovat, ale vždy musí být v jedné složce zapojeny nejméně dvě osoby s výjimkou složek v sekci „Volené orgány kraje“. Redaktorem pro každou složku je zpravidla jedna konkrétní osoba. Pracovníci útvarů nebo odborů předávají průběžně dle potřeby požadavky na školení k publikování na portálu pomocí RS e-mailem správci webu, který zajistí jejich proškolení v rozsahu, aby byli schopni samostatně publikovat požadovanou agendu.

Intranet systémově spravuje pověřený pracovník OI, který zajišťuje nastavení přístupů s příslušným oprávněním do jednotlivých webových částí intranetu. Na základě požadavků vedoucích odborů vytváří týmové weby jednotlivých odborů nebo pracovních skupin, proškolí správce příslušného týmového webu a metodicky jej vede.
Uživatelé intranetu mají jako výchozí oprávnění nastaveno „čtenář“ – mohou položky pouze číst, u diskusních webových částí jako „přispěvatel“ – mohou vkládat, upravovat a mazat položky. Vyšší oprávnění (přispěvatel, návrhář webu, správce) může přidělit správce intranetu na základě požadavku zaslaného na adresu sharepoint@kr-jihomoravsky.cz.
Vyšší oprávnění uživatelům do týmových webů odborů a pracovních skupin přidělují správci těchto webů.

4.4 Správce dokumentů JMK

Správce dokumentů JMK (dále jen „DMS“) je přístupný pouze po přihlášení.

Přístup do systému DMS umožní zaměstnanci JMK zařazenému do KrÚ pověřený pracovník OI na základě požadavku vedoucího příslušného odboru a po udělení souhlasu vedoucím OKH.

Automatický přístup do složek RJMK a ZJMK mají všichni VO, sekretariáty odborů, vedoucí ODORG, osoba pověřená zapisováním schůzí RJMK a zasedání ZJMK, ŘKrÚ, členové RJMK a jejich asistenti. Automatický přístup do složky ZJMK mají členové ZJMK a tajemníci politických klubů, automatický přístup do složky příslušné komise nebo výboru mají členové této komise nebo výboru a tajemníci příslušné komise nebo výboru. Všichni zaměstnanci JMK zařazení do KrÚ a všichni členové ZJMK, RJMK, výborů a komisí, jejich asistenti a tajemníci a tajemníci politických klubů mají přístup do výpisů usnesení z RJMK a ZJMK.

Každý žadatel o přístup do systému DMS je povinen vyplnit formulář „Souhlas s přístupem do systému Správce dokumentů JMK (DMS) provozovaného Jihomoravským krajem a prohlášení o zachování mlčenlivosti o osobních údajích v něm obsažených“, který je přílohou této směrnice. Vyplněný formulář včetně podpisu VO žadatel odevzdá před udělením souhlasu k přístupu do systému DMS na ODORG. Formulář není nutno vyplňovat v případě, že má příslušná osoba přístup pouze do složky výpisy usnesení.

Každá osoba s přístupem do systému DMS je povinna zachovávat mlčenlivost o osobních údajích v něm obsažených a tyto osobní údaje dále nezveřejňovat, nesdělovat nebo nezpřístupňovat třetím osobám. Povinnost zachovávat mlčenlivost o osobních údajích je upravena v ustanovení § 15 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

5 USTANOVENÍ PŘECHODNÁ A ZÁVĚREČNÁ

Toto vydání směrnice č. 11/INA-KrÚ nahrazuje předchozí vydání směrnice.

6 PŘÍLOHY

Příloha č. 1 formulář „Souhlas s přístupem do systému Správce dokumentů JMK (DMS) provozovaného Jihomoravským krajem a prohlášení o zachování mlčenlivosti o osobních údajích v něm obsažených“

Příloha č. 1 směrnice Provoz HW a SW - formulář „Souhlas s přístupem do systému Správce dokumentů JMK (DMS) provozovaného Jihomoravským krajem a prohlášení o zachování mlčenlivosti o osobních údajích v něm obsažených“

Jihomoravský kraj
Žerotínovo náměstí 3/5, 601 82 Brno

Souhlas s přístupem do systému Správce dokumentů JMK (DMS) provozovaného Jihomoravským krajem a prohlášení o zachování mlčenlivosti o osobních údajích v něm obsažených

Tímto prohlašuji, že souhlasím s přístupem do systému DMS provozovaného Jihomoravským krajem a beru na vědomí ustanovení § 15 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, které stanoví: „Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací“.

Fyzická osoba se může dopustit přestupku podle ustanovení § 44 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů tím, že poruší povinnost mlčenlivosti podle § 15 téhož zákona. Současně se fyzická osoba, která, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají nebo poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, vystavuje nebezpečí trestního stíhání pro trestný čin dle § 180 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Jméno a příjmení: ……..……..….

Adresa:…….

Kontakt:……

Funkce:…….

poskytl/a souhlas s výše uvedeným prohlášením a seznámil/a se s výše uvedenými skutečnostmi

dne ..... podpis .....

Souhlasím s přístupem do systému DMS výše uvedeného zaměstnance.

Podpis VO ……