Jihomoravský kraj Krajský úřad Jihomoravského kraje Žerotínovo náměstí 3 Brno	Interní normativní akt KrÚ směrnice **PROVOZ HW A SW**	Evidenční číslo	
		11/INA-KrÚ	
		Číslo vydání:	**9**
		Účinnost od:	**1.3.2018**

Pravidla používání výpočetní techniky, počítačové sítě a užívání software

OBSAH:

1 ÚVOD 2

1.1 Předmět a účel 2
1.2 Použité zkratky 2
1.3 Vymezení základních pojmů 2
1.4 Související předpisy 4

2 VÝPOČETNÍ TECHNIKA 5

2.1 Evidence výpočetní techniky 5
2.2 Základní pravidla práce s výpočetní technikou 5
2.3 Používání mobilní výpočetní techniky 6
2.4 Práce s datovými nosiči 7
2.5 Postup při předání, servisu a likvidaci VT 8

3 POČÍTAČOVÁ SÍŤ 8

3.1 Pravidla pro práci v lokální počítačové síti 8
3.2 Uživatelské jméno 9
3.3 Heslo 9
3.4 Centrální úložiště 9
3.5 Přemístění techniky 10
3.6 Hlášení závad a přidělování techniky 10
3.7 Fyzické zabezpečení výpočetní techniky 10
3.8 Antivirová ochrana 10
3.9 Zálohování dat 11

4 ELEKTRONICKÁ POŠTA A INTERNET 11

4.1 Pravidla používání elektronické pošty 11
4.2 Bezpečnost elektronické pošty 12
4.3 Přístup k internetu 12
4.4 Přístup k internetu pro návštěvy 13
4.5 Internetové stránky KrÚ 13
4.6 Správce dokumentů JMK 14

5 INFORMAČNÍ SYSTÉMY 15

5.1 Rozsah IS na KrÚ JMK 15
5.2 Pravidla pro používání IS KrÚ 15

6 USTANOVENÍ PŘECHODNÁ A ZÁVĚREČNÁ 16

7 PŘÍLOHY 16

ZPRACOVAL:	OVĚŘIL:	SCHVÁLIL:	ZÁVAZNÝ PRO:
OI	OI	JUDr., Roman Heinz, Ph.D. ŘKrÚ	KrÚ
Ing. Miroslav Vacula	Ing. Miroslav Vacula		
Datum a podpis: 16.2.2018 Miroslav Vacula, v. r .	Datum a podpis: 16.2.2018 Miroslav Vacula, v. r .	Datum a podpis: 16.2.2018 Roman Heinz, v.r.	

1 ÚVOD

1.1 Předmět a účel

Předmětem této směrnice je stanovení pravidel pro provozování výpočetní techniky, lokální počítačové sítě JMK, internetu, elektronické pošty a informačních systémů v rámci KrÚ.
Účelem tohoto dokumentu je zajistit bezpečné provozování výpočetní techniky, lokální počítačové sítě, internetu, elektronické pošty a informačních systémů výlučně oprávněnými uživateli, vysoká dostupnost informačních zdrojů, zamezení 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
HW	hardware
IS	informační systém
ISVS	informační systém veřejné správy
ISMS	Systém řízení bezpečnosti informací (Information Security Management System)
LAN	lokální počítačová síť (Local Area Network)
NB	notebook
ODHS	odd. hospodářské správy
ODORG	odd. organizační OKH
OMA	Outlook Mobile Access - podoba pro mobilní zařízení PDA, SmartPhone, Palm,..
OPVV	odd. personálních věcí a vzdělávání OKŘ
OI	odbor informatiky
OWA	Outlook Web Access – webový přístup k el. poště
PC	počítač (osobní počítač, Personal Computer)
SW	software
VPN	virtuální privátní síť
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 (dále IS) 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, pošta nebo účetnictví.

Správce sítě
Pracovník OI pověřený správou LAN.

Pracovník informatiky
Zaměstnanec OI.

Bezpečnostní správce odboru
Pracovník odboru, který zná problematiku informací na odboru a navrhuje jejich ochranu a zabezpečení.

ISMS
Je to proces zaměřený na zvládání informačních hrozeb, zajišťuje kontinuitu činností organizace, minimalizuje ztráty, maximalizuje návratnost investic, podporuje právní shodu a dobré jméno organizace.

Rozsah ISMS
ISMS se na KrÚ JMK vztahuje komplexně na oblast poskytování veškerých služeb občanům a organizacím, na veškeré procesy spojené s realizací těchto služeb i na procesy spojené se zajištěním řízení a správy organizace.

Správce SW
Pracovník informatiky pověřený správou a evidencí SW na KrÚ.

Správce IS
Pracovník, který na KrÚ uděluje uživatelská oprávnění, případně vytváří uživatelské účty a stará se o provoz IS.

Uživatel
Každý zaměstnanec, stážista, člen ZJMK, pracovník vykonávající práci na základě dohody o pracovní činnosti či dohody o provedení práce využívající IS jako nástroj k plnění pracovních povinností.

Uživatelský účet
Prostředek IS, který jednoznačně definuje uživatele a jeho oprávnění v daném IS. Je chráněný heslem.

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

Externí pracovník
Pracovník využívající prezentační techniku.

Datový nosič
Přenosné datové úložiště, které není fyzicky svázané s HW určené k pracovním účelům.

Software
SW lze rozdělit na systémový SW, který zajišťuje chod samotného PC 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). Zmíněný 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.

Mobilní výpočetní technikou jsou NB, chytré telefony - Smartphones, tablety a obdobné prostředky VT včetně periferních zařízení a příslušenství. Mobilní VT se používá pouze pro plnění pracovních povinností. Uživatelé mobilní VT mají právo ji používat jak v prostorách KrÚ, tak i mimo prostory KrÚ.

Uživatelem mobilní VT může být uživatel, jemuž byla mobilní VT přidělena do stálého užívání nebo uživatel, který o krátkodobou zápůjčku požádá prostřednictvím HelpDesku. Krátkodobé předání mobilní VT potvrdí uživatel podpisem v zápůjční knize na OI.

Cloud / Cloud computing
Je na internetu založený model vývoje a používání počítačových technologií. Lze ho také charakterizovat jako poskytování služeb či programů uložených na serverech na internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče nebo klienta dané aplikace a používat je prakticky odkudkoliv.
Cloud služby jsou například:

- mail servery (gmail, seznam, yahoo a další),
- disková uložiště (sdilej.cz, uloz.to, Dropbox, Google Drive a další),
- a další.

1.4 Související předpisy

- 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 pozdějších předpisů,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,
- 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce ,
- zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů,
- vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění vyhlášky č. 283/2014,
- vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů,
- vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění pozdějších předpisů,
- 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, ve znění pozdějších předpisů,
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů.

- *3/INA-KrÚ Spisový řád*
- *4/INA-KrÚ Podpisový řád*
- *9/INA-KrÚ Řízení dokumentace*
- *62/INA-KrÚ Bezpečnost informací*
- *34/INA-KrÚ Příručka kvality*
- *22/INA-KrÚ Poskytování práv k vyjmenovanému nehmotnému majetku*

2 VÝPOČETNÍ TECHNIKA

2.1 Evidence výpočetní techniky

V rámci platných právních norem a dokumentů KrÚ provádí základní evidenci zařízení VT OKŘ ODHS. VT jsou přidělena inventární čísla DDHM, resp. DHM. Rozšířenou evidenci zařízení VT včetně příslušenství vede OI ve specializovaném programu HelpDesk.

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 výpočetní techniky 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 dobu užití konkrétního SW a HW. U internetových prohlížečů dochází i k zaznamenávání navštívených webových stránek.

Při vypínání prostředků VT je třeba dodržet následující podmínky:
PC je povoleno vypínat prostředky operačního systému v režimech Vypnout, Režim spánku nebo Úsporný režim. Před vypnutím je nutné mít všechna data uložena. Vypínání síťovým tlačítkem lze použít pouze v případech, kdy nelze použít výše jmenované režimy. VT se zapíná a vypíná 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. Tiskárnu není dovoleno vypnout v průběhu tisku.

Uživatelé mají možnost tiskových výstupů na lokální a síťové tiskárny. Pokud je tiskárna připojena k PC a sdílena pro více uživatelů, není nutné pro zpřístupnění tisku přihlášení uživatele (stačí PC pouze zapnout). Je nutné v maximální možné míře používat oboustranný černobílý tisk. Tonery nebo cartridge k tiskárnám si uživatelé mohou vyměnit na OI vždy výměnou za prázdný kus. Výměnu tonerů v tiskárně provádí každý uživatel sám.

Na PC je možno používat pouze SW schválený a instalovaný pracovníky informatiky.

Osobě, která není zaměstnancem JMK zařazeným do KrÚ, popř. v poměru vyplývajícím ze zastávané funkce, je přístup k VT používané na KrÚ 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 jeho zástupce, pracovník informatiky, pracovník technického servisu nebo externí pracovník s povolením pracovníka informatiky.

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 mít rozpracovaná data uložena a 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),
- za 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,
- podrobně se seznamovat s pokyny pracovníků informatiky 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 VT,
- provádět systémové úpravy a změny HW a SW,
- samostatně povolovat sdílení prostředků PC (sdílení disků, složek, tiskáren atd.),
- používat na pracovišti jiné datové nosiče než datové nosiče vymezené v čl. 1.3. této směrnice,
- připojovat mobilní zařízení do počítačové sítě prostřednictvím WIFI s názvem „Zamestnanci“ v kancelářích. Toto připojení se smí používat pouze v zasedacích a školících místnostech. Dočasné připojení může schválit pracovník informatiky.

Uživatelé mohou používat služby počítačové sítě v pracovní dny od 6.00 do 20.00 hodin. Mimo tuto dobu není provoz sítě plně garantován, je 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

Uživatel mobilní VT je povinen:
- zabezpečit používanou mobilní VT a data na ní uložená proti odcizení a zneužití,
- 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).

Vzdálené připojení ke zdrojům KrÚ, ať pomocí OWA nebo VPN, může být aktivní jen po nezbytně nutnou dobu a nesmí být zpřístupněno neoprávněné osobě.

Minimálně jednou za 14 kalendářních dnů, pokud tomu nebrání zvláštní okolnosti (nemoc či jiná dlouhodobá nepřítomnost na pracovišti), musí být NB fyzicky připojen kabelem do počítačové sítě v budovách KrÚ z důvodu aktualizací SW, instalací opravných záplat a aktualizací antivirového programu. Při nedodržení této lhůty může být správcem zablokován účet daného NB v doméně.

Pracovníci informatiky 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.

Komunikační prostředky (telefon, tablet, smartphone) musí mít nastavené zabezpečení zařízení pomocí kódu PIN případně jiným vhodným bezpečnostním prvkem dle konkrétního zařízení. Ztráta těchto zařízení je vedena jako bezpečnostní událost a musí být neprodleně jako bezpečnostní událost nahlášena. Bude provedeno zablokování SIM a deaktivace/změna hesla u doménového účtu, kterým se z daného zařízení uživatel přihlašoval k poštovnímu serveru.

Šifrování mobilní VT – na požádání lze zašifrovat datové médium zařízení. Po zašifrování nelze bez šifrovacího klíče k datům přistupovat a riziko neoprávněného přístupu k datům se tím minimalizuje. O nutnosti tohoto šifrování rozhoduje uživatel nebo bezpečnostní správce odboru. O šifrovacím prostředku rozhoduje pracovník informatiky.

Na mobilních a komunikačních zařízení je zakázáno provádět jakékoliv zásahy, které by ovlivňovaly bezpečnost zařízení a dat, která jsou na nich uložena. Případné zásahy může provádět pouze pracovník informatiky:

- u notebooků nesmí dojít
    - k vypnutí antivirového programu a deaktivaci firewallu
    - přeinstalaci operačního systému zařízení
    - změně firmware
    - instalaci softwaru, který neschválí pracovník informatiky
- u chytrých mobilních telefonů a tabletů~~komunikačních prostředků~~ se doporučuje
    - používat antivirový program buď předinstalovaný od výrobce nebo doporučený pro konkrétní zařízení – s výběrem poradí pracovník informatiky
    - instalovat aktualizace programů a operačního systému

Případné požadavky na změny nastavení a instalace lze zadávat do systému HelpDesk.

2.4 Práce s datovými nosiči

Datové nosiče (zejména CD, DVD, flash disky) se využívají k výměně informací. Jejich odcizení, nebo ztráta je potencionálním nebezpečím úniku dat.
Z tohoto důvodu je třeba způsob výměny informací v rámci KrÚ prostřednictvím datových nosičů omezit na minimum a využívat bezpečnější způsoby, kterými jsou Intranet - Sharepoint server, sdílené složky na souborovém serveru nebo elektronická pošta.

Nepotřebné datové nosiče, CD, DVD a BlueRay disky lze zničit ve skartovacím zařízení na OI. Je nutné takto ničit všechna nepotřebné datové nosiče obsahující informace, u kterých je nutné zabránit jejich dalšímu šíření. Nahrané datové nosiče **musí** být označeny popisem, je-li to fyzicky možné a nebrání-li tomu jiné zákonné důvody.

2.5 Postup při předání, servisu a likvidaci VT

Data KrÚ musí být vhodným způsobem zabezpečena zejména v těchto případech:
- předání zařízení k užívání jinému uživateli mimo KrÚ,
- předání zařízení k fyzické likvidaci,
- předání zařízení do servisu,
- odprodej nebo darování zařízení.

Zálohování/odstranění dat uložených v zařízeních KrÚ je v kompetenci pracovníků informatiky pověřených touto činností.

3 POČÍTAČOVÁ SÍŤ

3.1 Pravidla pro práci v lokální počítačové síti

Doména počítačové sítě má název „kr-jihomoravsky“. Pro přístup do IS je nutné mít doménový uživatelský účet, který se získává na základě těchto pravidel:
- v případě pracovního poměru – účet vzniká i zaniká automaticky dle evidence v personálním IS. Automaticky vzniká i přístup do těchto IS – poštovní, personální, právní, souborový Portál úředníka, HelpDesk
- v případě jiného smluvního vztahu s JMK – účet vytváří a ruší na základě požadavku v IS HelpDesk správce sítě. Tento požadavek může vznést pouze přímý vedoucí daného pracovníka, bezpečnostní ředitel nebo ŘKrÚ. Tento účet nevzniká a nezaniká automaticky. Správce sítě oprávněnost požadavku kontroluje podle informací z OPVV. Zadavatel požadavku je odpovědný za zneplatnění takto vytvořených účtů a oprávnění, případně musí uvést dobu platnosti takového požadavku.

Vytváření uživatelských účtů do dalších IS a nastavení přístupových oprávnění provádějí správci IS na základě požadavku v IS HelpDesk. Zadavatel požadavku je odpovědný za zneplatnění takto vytvořených účtů a oprávnění, případně musí uvést dobu platnosti takového požadavku.

V případě nepřítomnosti uživatele musí být **včas** přijata taková organizační opatření, aby nebylo nutné přihlášení nepřítomného uživatele (např. přesměrování pošty, kopií souborů do sdílených složek atd.). **V žádném případě nezlze zpřístupnit uživatelský účet jinému uživateli.**
První pracovní den následující po dni ukončení pracovního poměru nebo odchodu na mateřskou dovolenou vypálí OI obsah složky uživatele v centrálním úložišti dat na datový nosič, které je k dispozici na OI a oproti podpisu jej může vyzvednout VO příslušného odboru nebo pověřená osoba a (automaticky se bere jako osoba pověřená pracovnice sekretariátu daného odboru). Podle potřeb lze vypálit i poštovní soubor *.pst (rozhoduje uživatel). Nevyzvednuté datové nosiče budou po uplynutí 3 měsíců od vypálení skartována.
Potvrzení o odebrání veškerých přístupových práv musí být v případě ukončení pracovního poměru součástí výstupního listu.
Správce sítě neumožňuje přístup takové VT do domény KrÚ, kterou KrÚ nevede v evidenci. Výjimku tvoří technika servisních organizací, kdy je přístup umožněn na základě smluvní dohody nebo po schválení správcem sítě.

3.2 Uživatelské jméno

Tvar uživatelského jména je: **prijmeni.jmeno** (výjimku tvoří servisní účty a účty určené pro školení uživatelů), kde **„prijmeni“** je příjmením uživatele a **„jmeno“** je křestní jméno uživatele. U jmen příliš dlouhých je křestní jméno zkráceno. Shoda jmen se řeší individuálně.

3.3 Heslo

K uživatelskému jménu přináleží heslo. Prvotní (dočasné) heslo při zřízení účtu stanoví správce IS a uživatel ho musí při prvním použití změnit. Konvence pro zadávání hesla:
minimální délka hesla je 8 znaků, heslo musí být kombinací velkých písmen, malých písmen a musí obsahovat alespoň jeden speciální znak nebo číslici a nesmí obsahovat část uživatelského jména a diakritiku. Platnost hesla je 100 dnů.
Příklad správně utvořeného hesla: kx7V#PpB.

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. Uživatel nese plnou zodpovědnost za prozrazení (tím je myšleno i sdělení hesla jinému pracovníkovi KrÚ), odcizení, ztrátu a zneužití hesla. Nadřízený pracovník nesmí požadovat po uživateli sdělení hesla k jeho uživatelskému účtu. Doménová politika je nastavena tak, že třetí chybně zadané heslo uzamkne uživatelský účet na 60 minut. Účet může před vypršením tohoto intervalu odemknout správce sítě na žádost uživatele. V případě, že uživatel své heslo zapomene, požádá správce sítě o jeho změnu. Správce sítě v takovém případě nahradí stávající heslo uživatele dočasným heslem, které je nutné následně uživatelem změnit. Některé IS, 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 Centrální úložiště

Centrální úložiště je v síti KrÚ provozováno na souborovém serveru připojeném k diskovým polím. Na tomto úložišti se ukládají data uživatelů, odborů a pracovních skupin.

Složka uživatele – mapovaný disk H (Home)
Běžně zpracovávaná data je uživatel povinen ukládat na disk H**,** který je směrován na uživatelovu složku v centrálním úložišti. Pokud uživatel neuloží svá data v centrálním úložišti, nese plnou odpovědnost za jejich ztrátu. Složka uživatele **nesmí být použita pro ukládání dat nesouvisejících s pracovní náplní,** např. hudby, soukromých obrázků, fotografií apod.

V případě, že se jedná o data svým obsahem citlivá, musí uživatel tato data šifrovat (chránit heslem nebo jiným podobným prostředkem), případně se poradit s bezpečnostním správcem o vhodném uložení těchto dat. O citlivosti dat rozhoduje uživatel.
Uživatel má k této složce výhradní přístup, ale lze do ní na základě požadavku vedoucího umožnit přístup dalším uživatelům. O rozsahu přístupu musí být uživatel informován**.** Na tomto disku je nastavena tzv. disková kvóta -povolený objem ukládaných dat.

Data odborů a oddělení - mapovaný disk O (Odbory)
Tato složka je přístupná pouze pracovníkům daného odboru nebo oddělení a slouží k ukládání sdílených dat tohoto odboru nebo oddělení. O přístupová práva uživatelů mimo daný odbor nebo oddělení může požádat prostřednictvím požadavku v IS HelpDesk vedoucí daného odboru nebo oddělení. Uživatelům mimo hlavní pracovní poměr nevzniká přístup automaticky. Je nutné dbát na citlivost ukládaných dat. Součástí mapovaného 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 správcem sítě odstraněna**. Je nutné dbát na citlivost ukládaných dat.

Skupiny
V centrálním uložišti lze vytvářet složky s individuálním přístupovým oprávněním pro pracovní skupiny. Přiřazení přístupových práv a umístění sdílené složky nastavuje pracovník informatiky pouze na základě požadavku v IS HelpDesk.

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 informatiky a jejich kopii mohou ukládat lokálně na svých PC.

3.5 Přemístění techniky

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

3.6 Hlášení závad a přidělování techniky

Závady na VT je povinen uživatel neprodleně hlásit na OI dle pokynů uvedených v *příloze č. 2 této směrnice*. 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 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.

3.7 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, s odkazem na bezpečnostní politiku KrÚ a normu ISO 27001. Místnosti, kde jsou umístěny servery a uloženy zálohy dat, musí být kromě prvků pasivní bezpečnosti zabezpečeny také prvky aktivní bezpečnosti – elektronickou požární signalizací, elektronickou zabezpečovací signalizací a logováním přístupu do místnosti. Místnosti, kde jsou umístěny aktivní prvky LAN, musí být kromě prvků pasivní bezpečnosti zabezpečeny také elektronickou požární signalizací. Nutnost instalace elektronické zabezpečovací signalizace bude posouzena pro každý jednotlivý případ zvlášť.

3.8 Antivirová ochrana

Antivirový systéme musí být instalován na každé zařízení, které takovou instalaci umožňuje. Antivirový program instaluje a konfiguruje odpovědný pracovník informatiky. Na NB je instalována antivirová ochrana včetně firewallu. Aktualizace antivirových programů je pro PC

připojené k počítačové síti prováděn automaticky. Na PC nepřipojených do sítě internet provádí update pověřený pracovník informatiky. Uživatel, který zjistí, že je jeho PC zavirován nebo že obdržel zavirovanou poštu, uvědomí o tomto faktu pracovníky informatiky. 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 je proto doporučeno ponechat ve středu při odchodu z práce PC zapnutý a odhlášený. Pokud tak neučiní, bude antivirová kontrola provedena automaticky při nejbližším zapnutí PC.

3.9 Zálohování dat

Tato problematika je řešena pracovním postupem na OI.

4 ELEKTRONICKÁ POŠTA A INTERNET

4.1 Pravidla používání elektronické pošty

Poštovní server
- KrÚ provozuje vlastní poštovní server, kde je uložen obsah všech poštovních schránek, dále pak veřejné složky a globální adresář.
- Poštovní server je v pravidelných intervalech zálohován.
- Příchozí elektronická pošta je kontrolována antivirovým programem a prohlédnuta antispam filtrem. Konfigurace těchto IS zajišťuje pracovník informatiky.
- K elektronické poště lze přistupovat ze sítě internet přes webový odkaz https://email.kr-jihomoravsky.cz. V případě mobilní VTprovádí nastavení pracovník informatiky.
- O poštovní server se stará pracovník informatiky.

Poštovní schránka
- Schránka elektronické pošty je chráněna doménovým uživatelským účtem.
- Formát adresy osobní poštovní schránky je **prijmeni.jmeno@kr-jihomoravsky.cz.** Ve výjimečných případech se určí jiná adresa (délka jména, shoda jmen atd.).

Na serveru jsou 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. Postup zpracování elektronických podání stanoví směrnice č. *3/INA-KrÚ Spisový řád.*
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). Maximum adresátů pro venkovní adresy (mimo doménu kr-jihomoravsky) je 100. Za překročení limitu odpovídá odesílatel. Za naplněnost 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 poštovní schránky povoluje pracovník informatiky.

Uživatelé elektronické pošty jsou povinni nezneužívat elektronickou poštu pro mimopracovní účely (viz 2.2).
Zaměstnavatel využívá ke kontrole veškeré elektronické pošty antispamový SW (GFI MailEssentials). Zprávy vyhodnocené jako spam jsou podle nastavených kritérií zpracovány

a dále buď odeslány uživateli, zařazeny do nevyžádané pošty nebo uloženy do karantény na serveru S-GFI. O uložení zprávy do karantény je adresát informován automaticky zaslanou zprávou z programu GFI MailEssentials. S těmito zprávami může pracovat dle návodu zveřejněném na Interním portále úředníka. Při čtení elektronické pošty je třeba 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.).
V případě vícedenní nepřítomnosti je uživatel povinen použít tzv. „Službu mimo kancelář“ a v případě nutnosti pomocí „Průvodce pravidly...“ nastavit přeposílání kopie zpráv na jiného pracovníka, případně mu prostředky poštovního klienta (Outlook) 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.*

4.2 Bezpečnost elektronické pošty

Informace posílané elektronickou poštou nejsou nijak chráněny proti odposlechu a mohou být velmi snadno po cestě zachyceny. Zajištění důvěrnosti informací lze provést formou zaheslování příloh nebo šifrováním zpráv.

Uživatelům je zakázáno rozesílat elektronickou poštou zprávy s jakoukoliv přílohou pomocí distribučního seznamu „všem z KrÚ JMK“ – k tomu lze využít prostor na Interním portále úředníka.
Pracovník informatiky pověřený správou elektronické pošty je oprávněn konfigurovat systém tak, aby snížil riziko doručení nebezpečných zpráv uživatelům, například filtrací, nebo blokováním odesilatelů.
Vzhledem k tomu, že elektronická pošta úřadu není určena pro nepracovní účely, může KrÚ 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 s plným respektováním příslušných zákonných úprav včetně soudní judikatury či stanovisek Úřadu pro ochranu osobních údajů. Přesměrování nebo sdílení elektronické pošty z osobní schránky uživatele na jinou adresu je možné pouze na žádost uživatele osobní schránky.

Pro archivaci vybraných schránek 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.
Je **zakázáno** nastavení automatického **přeposílání** e-mailů na e-mailové adresy mimo síť Jihomoravského kraje.

4.3 Přístup k internetu

Připojení LAN do prostředí internetu je zabezpečeno firewallem (zabezpečení počítačové sítě proti útokům z internetu), na mobilní VT 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 UTM. 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. Veškeré přístupy na internet jsou monitorované. Pravidla přístupu zabezpečuje OI. Uživatelé internetu jsou povinni:

- internet používat výhradně k plnění pracovních povinností (viz 2.2) 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 informatiky se zakazuje:
- měnit nastavení a konfiguraci připojení do internetu s výjimkou mobilní VT,
- stahovat z internetu jakýkoliv SW (včetně zdarma nabízeného SW),
- 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 informatiky, pokud to dovolí velikost stahovaných dat a technické možnosti,
- přijímat pomocí internetu radiové a televizní vysílání (s výjimkou pracovníků, u nichž to vyžaduje pracovní náplň),
- pracovat s internetem jakýmkoliv způsobem, který by porušoval platné zákony, právní úpravy a interní předpisy KrÚ.

Uživatelům se zakazuje:
- využívat Cloud služby (pozor na aplikace využívající cloudových řešení např. Office 365, DropBox) v síti internet pro ukládání krajských dat bez předchozího schválení pracovníkem informatiky. Schválení nepodléhá využití nabízených internetových služeb na Interním portálu úředníka. Při ukládání krajských dat je nutné dbát na citlivost uložených dat, kdy uložením dat na Cloud dává uživatel data k dispozici provozovateli konkrétní Cloud služby (v závislosti na smluvních a licenčních podmínkách, se ukládaná data mohou stát majetkem poskytovatele Cloud služby). Za zneužití zodpovídá uživatel.

Důvodem výše uvedených zákazů je zejména zajištění bezpečnosti LAN, dodržování právních norem a zajištění dostatečné propustnosti připojení do internetu (omezená šíře pásma).Přístup k internetu pro návštěvy
Je k dispozici WIFI síť s SSID názvem „wifijmk“. Přes toto připojení nelze přímo vstupovat do vnitřní sítě JMK. Slouží pouze pro přístup k internetu.

4.4 Internetové stránky KrÚ

KrÚ provozuje tyto typy internetových stránek:
- Webový portál JMK – oficiální veřejný portál JMK a KrÚ přístupný všem uživatelům internetu (https://www.kr-jihomoravsky.cz).
- Intranet - portál úředníka přístupný pouze uživatelům s účtem v AD (http://urednik.kr-jihomoravsky.int).
- Extranet – portál přístupný z veřejné internetové sítě pouze po přihlášení (https://www.kr-jihomoravsky.cz/dms).

Webové stránky portálu systémově spravuje pověřený pracovník informatiky – správce webových stránek. Zajišťuje jejich vývoj, nasazení, funkčnost a přípravu grafických šablon. Udržuje redakční systém pro vkládání a administraci dat, správu uživatelů a jejich oprávnění podle rolí a struktury složek stejně jako školení odpovědných osob za publikování. Na intranetu na Interním portále úředníka ve veřejné části dokumentů OI se v sekci Publikační systém zveřejňuje a aktualizuje seznam osob zapojených do redakčního systému, 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 VO 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 redakčním systému 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 redakčního systému e-mailem správci webu, který zajistí jejich proškolení v rozsahu, aby byli schopni samostatně publikovat požadovanou agendu.

Intranet systémově spravuje pověřený pracovník informatiky, 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 HelpDesk.
Vyšší oprávnění uživatelům do týmových webů odborů a pracovních skupin přidělují správci těchto webů.

4.5 Správce dokumentů JMK

DMS je přístupný pouze po přihlášení na adrese http://www.kr-jihomoravsky.cz/dms.
Přístup do systému DMS umožní zaměstnanci JMK zařazenému do KrÚ pověřený pracovník informatiky na základě požadavku vedoucího příslušného odboru a po udělení souhlasu vedoucím ODORG.

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 k přístupu 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 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 INFORMAČNÍ SYSTÉMY

5.1 Rozsah IS na KrÚ JMK

V prostředí KrÚ je provozována řada IS, které umožňují vykonávat a řešit jednotlivé agendy, potřeby a plnit zákonné povinnosti úřadu. Řada z nich je vzájemně propojena. Mezi klíčové patří IS GINIS, který řeší agendu spisové služby, podatelny, ekonomické agendy (evidence a oběh ekonomických dokladů, včetně smluv a objednávek) a napojení na externí systémy a registry, jako jsou ISDS, ISRS, CzechPoint, el. bankovnictví.
K dalším významným IS se řadí FLUX, řešící agendu mzdovou, personální, evidenci docházky, stravenek, IS ATTIS (směrnice, organizační struktura) a další.

5.2 Pravidla pro používání IS KrÚ

Základní (obecný) přístup do IS KrÚ získá uživatel současně se vznikem (vytvořením) doménového uživatelského účtu. Specifický přístup související s konkrétní pracovní náplní zaměstnance, získá uživatel teprve na základě požadavku vytvořeného v HelpDesku. Požadavek na oprávnění do konkrétní agendy (spisová služba, ekonomika, specifická oprávnění) v ideálním případě zadává nadřízený zaměstnance.

5.2.1 Ověřování uživatele

Ověření uživatele pro přístup do IS nebo aplikace probíhá formou tzv. autentizace a autorizace. V případě tzv. Windows autentizace se jedná o ověření uživatele proti jeho doménovému účtu. Některé IS (např. GINIS, ATTIS) stačí spustit, ověření uživatele probíhá na pozadí. V případě dalších IS a aplikací je nutné doménové jméno vypsat. Do řady specifických agend (aplikací) je přístup řešen pomocí jedinečného účtu založeného v databázi (např. INISOFT, ELEGIS, ZORRO), kde je nutné přihlašovací údaje vyplnit. Současně přihlašovací údaje nepodléhají doménové bezpečnostní politice, tj. heslo je stále platné a přístupové údaje spravuje konkrétní správce.

5.2.2 Kompetence pracovníků informatiky

OI, resp. konkrétní správce IS nebo aplikace odpovídá za dostupnost systému, aktivní přístupové údaje a patřičný rozsah přístupových oprávnění uživatele. Tím je myšleno rozsah modulů a jejich vhodná parametrizace (na základě požadavku nebo specifické náplně funkčního místa). OI dále odpovídá za zálohování IS a pořizovaných (vzniklých) dat. OI vytváří a navrhuje koncepci IS takovým způsobem, aby byla v souladu s legislativou a plnila požadavky odvětvových odborů. Odvětvové odbory se mohou na OI obracet s požadavky na změnu, rozšíření nebo pořízení konkrétního řešení a OI navrhne způsob, jak daný požadavek zakomponovat do již existující architektury jednotlivých IS a řešení.

5.2.3 Metodická podpora

Požadavky na metodickou podporu vyhodnocují metodici jednotlivých odborných oblastí (např. metodickou podporu v oblasti spisové služby poskytují pracovníci OKŘ, podporu v oblasti ekonomiky pracovníci OE). Pracovníci OI řeší metodickou podporu IS jen rámcově, v žádném případě nejsou oprávnění a kompetentní po odborné stránce určovat, co je vhodným metodickým postupem.“

5.2.4 Způsob hlášení požadavků a poruch

Požadavky a hlášení poruch se provádí výhradně přes HelpDesk. Výjimku tvoří požadavky na nedostupnost některého z klíčových IS nebo aplikací, HW nebo sítě. V takovém případě se uživatelé mohou na OI obracet telefonicky.

5.2.5 Reakční doby řešených požadavků

Výčet reakčních dob, termíny řešení jednotlivých požadavků a další informace o prioritách a způsobu zadávání problémů vymezuje *příloha č. 2 Fungování IT podpory a provoz Helpdesku.*

6 USTANOVENÍ PŘECHODNÁ A ZÁVĚREČNÁ

Deváté vydání této směrnice 11/INA-KrÚ nahrazuje osmé vydání směrnice 11/INA-KrÚ účinné od 01.01.2017 do 31. 1. 2018.

7 PŘÍLOHY

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

Příloha č. 2 fungování IT podpory a provoz HelpDesku