FAKULTNÍ NEMOCNICE OLOMOUC
I. P. Pavlova 185/6, 779 00 Olomouc
☎ + 420 588 441 111, e-mail: info@fnol.cz

METODICKÝ POKYN č. MP-I001-03

Pravidla a postupy pro uživatele při používání prostředků ICT

1. vydání ze dne: 11. 7. 2016
Účinnost od: 11. 7. 2016

Skartační znak: A
Stupeň důvěrnosti: N1

	Jméno	Funkce	Datum	Podpis
Odborný garant	Ing. David Miklík	vedoucí Odboru informatiky		
Schválil	Ing. Antonín Hlavinka	náměstek informačních technologií		

1 ÚVODNÍ USTANOVENÍ

1.1 Účel

1.1.1 Metodický pokyn stanovuje závazná pravidla a postupy pro uživatele při používání prostředků ICT, které jsou součástí IS FNOL. Slouží k zajištění bezproblémového, řádného a bezpečného chodu prostředků ICT, předepisuje řádné nakládání s prostředky ICT. Upravuje technické a organizační podmínky pro ochranu dat.

1.2 Závaznost

1.2.1 Tento metodický pokyn je závazný pro všechny uživatele prostředků ICT.

1.3 Správa normy

1.3.1 Správa normy se řídí směrnicí Sm-G001 Vznik a řízení organizačních norem.

2 VYMEZENÍ POJMŮ

2.1 Zkratky

FNOL	Fakultní nemocnice Olomouc
ICT	Informační a komunikační technologie
IS	Informační systém
LF UPOL	Lékařská fakulta Univerzity Palackého v Olomouci
OINF	Odbor informatiky
OS	Operační systém
PC	Osobní počítač
SW	Software
UIT	Úsek informačních technologií

2.2 Definice

2.2.1 Prostředky ICT jsou veškeré technologie a nástroje, které uživatelé používají pro komunikaci a práci s informacemi (sdílení, distribuce a sběr informací, ukládání, vyhledávání, manipulace, přenášení nebo příjem - PC, tablety, mobily, aplikace, IS…) a ke komunikaci mezi sebou prostřednictvím počítačů nebo propojených počítačových sítí.

2.2.2 Počítačová síť slouží ke komunikaci a propojení počítačů za určitých pravidel, umožňuje uživatelům sdílení informací. Počítačová síť je souborem prostředků, zajišťujících komunikaci mezi počítači. Pokud není uvedeno jinak je v dokumentu pod pojmem síť, myšlena počítačová síť.

2.2.3 Informační systém (IS) je souhrn všech prostředků ICT zajišťujících pořízení, uchovávání a využívání datových informací.

2.2.4 Programové vybavení (software, program, aplikace) je sada všech počítačových programů a elektronických instrukcí, které říkají počítači, co má dělat, které mají nějakou funkci a vykonávají určitou činnost. Software sám je vždy nehmotný, ke svému šíření a používání vždy potřebuje prostředky výpočetní techniky. Jednotkou (částí) programového vybavení, obvykle řešící určitou problematiku, je aplikace (klinický informační systém KIS, PACS, personální IS VEMA, ekonomický IS, apod.).

2.2.5 Operační systém je základní programové vybavení počítače (tj. software), které je prostředníkem mezi hardwarem a aplikačním softwarem. Ve své podstatě je to soubor programů, díky kterým můžeme počítač ovládat. Zavádí se do paměti počítače při jeho startu a zůstává v činnosti až do jeho vypnutí.

2.3 Odborné funkce

2.3.1 **Správce prostředků ICT** - odborný útvar, který zajišťuje provoz prostředků ICT. Ve FNOL je tímto odborným útvarem OINF, případně UIT, jehož součástí OINF je.

Zajištěním provozu se rozumí soubor činností, které zajišťují funkčnost IS (odstranění nebo zamezení vzniku chybových stavů IS). Správce prostředků ICT dále monitoruje optimální využívání, navrhuje vedení FNOL rozvoj a potřebné úpravy, školí vybrané zaměstnance, přijímá od uživatelů požadavky a připomínky na provoz prostředků ICT. Spravuje uživatelské účty vč. e-mailových adres, zodpovídá za správné nastavení parametrů v programech, instalaci systémového SW, bezpečnostní politiky provozu ICT atd.

Některé činnosti zajišťující funkčnosti ICT je oprávněn provádět i proškolený pracovník, který není pracovníkem UIT/OINF (např. místní správce, klíčový uživatel, odborný garant…), ale pouze v rozsahu svého proškolení a oprávnění.

2.3.2 **Uživatel** - je fyzická osoba, které jsou přiděleny správcem prostředků ICT uživatelské přístupy do počítačové sítě FNOL.

3 VLASTNÍ TEXT

3.1 Zásady pro uživatele ICT ve FNOL

3.1.1 Základní informace a zásady

Přístup do sítě je povolen pouze uživatelům, kteří mají v rámci FNOL zřízen účet. Je zakázáno umožnit přístup osobám, které účet zřízen nemají, které nemají právo získat účet, nebo kterým byl účet zablokován, či zrušen.

Práci v síti zahajuje pracovník přihlášením se do ní, čímž jsou mu zpřístupněny prostředky a služby dané jeho uživatelským oprávněním.

Uživatel smí používat pouze přístupová práva, která mu řádným způsobem náležejí, a nesmí vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel jakýmkoliv způsobem získá přístupová práva, která mu nebyla přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci prostředků ICT. Takto získaná práva nesmí použít.

Uživatel smí pracovat na PC pracovišti sítě FNOL pouze pod uživatelským jménem a heslem jemu přiděleným, heslo ke svému uživatelskému jménu udržuje v tajnosti tak, aby bylo zabráněno jakékoliv možnosti zneužití. Výjimku tvoří PC pracoviště s automatickým přihlašováním pod "obecným uživatelem".

Uživatel smí pracovat v programovém vybavení (aplikaci) pouze pod uživatelským jménem a heslem jemu přiděleným, heslo ke svému uživatelskému jménu udržuje v tajnosti tak, aby bylo zabráněno jakékoliv možnosti zneužití.

U aplikací, které umožňují autentizaci uživatele při přihlášení do aplikace pomocí Active Directory, je přihlašování nastaveno výhradně tímto způsobem. Uživatel se do této aplikace tedy hlásí stejným uživatelským jménem a heslem, kterým se přihlašuje do počítačové sítě.

Uživatel zodpovídá za škody vzniklé v důsledku zneužití jeho účtu zaviněné nedbalou manipulací s účtem.

Uživatel je povinen se chovat tak, aby jeho činnost jen v minimálním rozsahu negativně ovlivňovala možnosti využití prostředků ICT dalšími uživateli. To se týká jak neúměrného

zatěžování linek v době jejich maximálního využití, tak i neúměrného zatěžování jednotlivých počítačů. Všechny takovéto činnosti je vhodné konzultovat se správcem prostředků ICT a řídit se dále jeho pokyny.

Při zjištění porušení zásad stanovených touto směrnicí, nebo při podezření ze zneužívání sítě FNOL je povinností uživatele okamžitě informovat správce prostředků ICT.

Uživatel má právo užívat prostředky počítačové sítě (jako diskový prostor, výkon procesoru, kapacitu přenosových linek, apod.) pouze s ohledem na celkové zatížení systému nebo sítě. Uživatel musí neprodleně uposlechnout pokynů administrátora na snížení jím generované zátěže.

Uživatel má právo využívat jemu přidělený vymezený diskový prostor. Současně odpovídá za jeho efektivní využití, obsah a objem dat. Zjevně nepracovní data budou správcem prostředků ICT bez varování a nekompromisně odstraňována.

3.1.2 Uživatelům ICT je zakázáno

Využívat prostředky ICT, které jsou majetkem FNOL a jsou součástí IS FNOL pro soukromou potřebu.

Kopírovat programové vybavení nebo data, k nimž FNOL vykonává vlastnická práva, resp. Práva k užívání.

Provádět neautorizovanou modifikace programů, dat nebo technického vybavení v majetku či užívání FNOL, zvlášť přísně jsou pak zakázány neautorizované změny konfigurace počítačů či jiných prostředků, které by mohly mít vliv na provoz celé počítačové sítě.

Úmyslně poškozovat nebo ničit prostředky ICT (např. počítačů, programového vybavení, komunikačních linek atd.).

Odposlouchávat provoz a vytvářet kopie zpráv či dat procházejících jednotlivými uzly sítě.

Používat prostředky ICT FNOL k činnostem uvedených v předchozích bodech namířených proti jakékoliv další organizaci, jejíž ICT jsou dostupné prostřednictvím počítačové sítě nebo sítě internet.

Sdělovat své přístupové heslo do sítě jiným osobám, je povinen toto heslo udržovat v tajnosti.

Zneužít nedbalosti jiného uživatele (např. opomenuté odhlášení) k tomu, aby v síti pracoval pod cizí identitou.

Obcházet bezpečnostní funkce.

Vědomě používat v síti prostředky ICT nakažené viry nebo jinými škodlivými kódy.

Přerušovat a bránit operačnímu systému a instalovanému SW v provádění automatických aktualizací.

Přerušovat a bránit monitoringu využití PC ve sběru dat.

Přerušovat a bránit antivirovému programu při kontrole systémů a provádění automatických aktualizací.

Instalovat programy nebo technická zařízení, která monitorují činnost jiných uživatelů nebo serverů, případně jinak zasahovat do oblasti sítě.

Provádět technické zásahy do konfigurace zařízení sítě a pracovních stanic nebo zaměřovat jejich jednotlivé komponenty.

Svévolně instalovat a používat neevidované programové vybavení, nebo instalační soubory neevidovaných programů ukládat na pevném disku, instalovat jakékoliv hry či hrát je na síti internet.

Šířit, nebo se snažit získat nelegální software.

Přetěžovat síť bezdůvodným přenášením dat o velkém objemu.

Používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům.

Je zakázáno používat síť pro politickou, náboženskou a rasovou agitaci.

Je zakázáno stahování (downloading) dat nebo programů o velkém objemu (filmy, obrázky, hudba, velké texty, apod.), pokud tyto nesouvisejí přímo s plněním pracovního úkolu.

Stahovat, ukládat nebo distribuovat soubory, které nesouvisí s jeho funkčním zařazením a pracovní náplní.

Provádět jakoukoliv činnost, která by mohla ohrozit provozuschopnost nebo bezpečnost pracovní stanice nebo počítačové sítě.

Využívat sítě FNOL ke komerčním účelům, nebo rozesílat nevyžádanou poštu (SPAM).

Jakkoliv mechanicky manipulovat s výpočetní technikou, s výjimkou výměny papíru, toneru a cartridgí v tiskárně. Zejména vypojovat, přepojovat, nebo demontovat komponenty počítače (monitor, klávesnice, myš, tiskárna), vypojovat počítač z počítačové sítě, rozpojovat nebo přerušovat počítačovou síť, připojovat k počítačové síti nebo k počítači jiné počítače nebo zařízení. Některé speciální úkony jsou svěřeny místnímu správci.

Připojovat zařízení k počítači, nebo další prostředků ICT k síti.

Uvádět do provozu a provozovat servery napojené na lokální síť. Týká se to zejména serverů služeb WWW, FTP.

Používat počítače jinak než k činnostem přímo souvisejícím s pracovní činností. Zejména se to týká hraní her a komunikace prostřednictvím internetu a různých webových či e-mailových chatů, apod.

Provozovat činnosti související s možností neoprávněného proniknutí do ochrany místního nebo cizího počítačového systému nebo odhalení hesel jiných osob (nejen uživatelů místní sítě) uchovávat data nebo programy, které jsou k této činnosti určeny, odposlouchávat provoz na přenosových mediích sítě (tedy data přenášená mezi jednotlivými počítači prostřednictvím počítačové sítě).

Provádět změny konfigurace prostředků ICT nebo zásahy do jejich systémů. Za případné škody napáchané uživatelem odpovídá v plné výši uživatel sám.

Provádět jakékoli akce, které vedou k narušení dat jiného uživatele, a to i v těch případech, kdy uživatel svá vlastní data explicitně nechrání.

Kopírovat jakákoliv data nebo programy z uživatelských adresářů bez souhlasu jejich majitelů (to zahrnuje i samotné prohlížení těchto adresářů). Toto omezení platí i v případě, že uživatelské adresáře jsou svými majiteli ponechány volně přístupné elektronickými prostředky.

Uživatel nesmí žádným způsobem zveřejňovat informace, či soubory dat, které by mohly vést k poškození ochrany sítě, programů nebo FNOL. Za zveřejnění se považuje zejména jejich neautorizované kopírování, vystavení na místních nebo jiných WWW serverech, jejich zasílání elektronickou poštou, apod.

Kopírovat nebo zálohovat data, která obsahují osobní údaje bez souhlasu vedení FNOL, vynášet či posílat tato data mimo prostory FNOL bez předchozího souhlasu vedení FNOL.

Využívat elektronických prostředků (především elektronickou poštu) k obtěžování nebo zastrašování jiných uživatelů. Do této kategorie spadá i rozesílání řetězových dopisů či dopisů na náhodně vybrané adresy v síti

Využívat počítačové prostředky FNOL k páchání trestných činů.

Používat počítačovou síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných organizací).

Manipulovat (přemísťovat, nastavovat, přenášet) s jednotlivými PC stanicemi a zařízeními.

Připojovat do sítě FNOL jakékoliv jiné elektronické zařízení, které není majetkem FNOL (notebooky, tiskárny, modemy, atd…).

Používat jakékoliv přenosné zařízení či nosič dat obsahující tzv. systémové bootovací soubory, nebo SW, čímž se rozumí přenosné HDD, flash paměti, diskety, apod.

Aktivně vytvářet nebo šířit škodlivý SW, znemožňovat funkci ochranného SW.

Otevírat či ukládat na diskový prostor jakýkoliv soubor neznámého původu (získaný na datovém médiu, elektronickou poštou či jiným způsobem). Má-li uživatel podezření z nakažení (nikoliv obdržení) svého PC virem, neprodleně informuje správce prostředků ICT.

Znemožňovat správci ICT jakýmkoliv způsobem vzdálený přístup k prostředkům ICT.

3.1.3 Uživatel je povinen:

a) Používat prostředky ICT pouze k účelům, ke kterým jsou určeny.
b) Dodržovat stanovenou heslovou politiku (viz. odst. 3.2.).
c) Dodržovat bezpečnostní zásady práce v počítačové síti FNOL a na přiděleném zařízení.
d) Používat pouze SW schválený a instalovaný správcem ICT.
e) Umožnit správci ICT vzdálenou správu přiděleného počítače a na požádání spolupracovat při obnovení standardního stavu pracovní stanice.
f) Antivirovým programem testovat stahované soubory, kontrolovat používané nosiče při jejich vkládání a vyjímání.
g) Při virové nákaze nebo neobvyklém chování zařízení ICT okamžitě jej vypnout a tuto skutečnost neprodleně nahlásit správci sítě.
h) Při jakémkoliv opuštění PC pracoviště toto pracoviště zabezpečit proti zneužití tzv. zamčením počítače (klávesová zkratka Win+L).
i) Průběžně zálohovat veškerá data uživatele, která nejsou uložena na síťových discích. Správce ICT neodpovídá za případnou ztrátu uživatelských dat, které nebyly řádně zálohovány.
j) Zálohovat lokálně uložená uživatelská data.
k) Dodržovat zásady FNOL při zpracování, ukládání a manipulaci s daty.
l) Při komunikaci s jinými sítěmi je uživatel povinen dodržovat pravidla, která platí v těchto sítích.

3.2 Heslová politika

3.2.1 Pro používání hesel platí zejména tato pravidla:

a) Heslo musí být uchováno v tajnosti a zodpovědnost za všechny činnosti, související s použitím identifikátoru a hesla, má jeho vlastník.
b) Heslo musí být zvoleno tak, aby nebylo snadné je odhalit, tj. musí být vytvořeno dle následujících pravidel:
   - minimální délka hesla je 12 znaků pro uživatele, pro administrátora 17 znaků,
   - musí obsahovat alespoň jedno malé písmeno (a-z)
   - musí obsahovat alespoň jedno velké písmeno (A-Z)
   - doporučuje se používat alespoň jednu číslici
   - doporučuje se neužívat znaků „y, y“ a „z, z“
   - heslo nesmí obsahovat osobní číslo, jméno a příjmení uživatele
   - je zakázáno tvořit hesla na základě mnohonásobně opakujících se znaků
   - nedoporučuje se používat, jména nebo čísla spojená s uživatelem (rodná čísla, jména dětí apod.), a to ani jejich kombinace.
   - je zakázáno opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel
c) Heslo k vlastnímu účtu uživatel nesmí sdělit druhé osobě.
d) Povinná změna hesla v intervalu maximálně po 18 měsících
e) Povinná změna hesla pokud existuje možnost, že mohlo být vyzrazeno.
f) Uživatelské jméno a heslo použité v síti a aplikacích FNOL je zakázáno používat v aplikacích mimo FNOL (sociální sítě, diskusní fóra apod.).
g) Nedoporučuje se zapisovat svoje heslo na papír. Pokud je heslo zapsáno, musí být bezpečně uschováno např. v zalepené obálce v trezoru.

h) Nedoporučuje se použití funkcí a programů pro zapamatování hesel, použití kombinace kláves pro vyvolání hesla apod.
i) V případě, kdy jsou dodávány technické nebo programové prostředky s heslem nastaveným výrobcem, musí být toto heslo okamžitě po převzetí (instalaci) změněno.
j) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností uživatele změnit toto heslo při prvním přihlášení.
k) Uživatel si musí být vědom toho, že oprávnění zaměstnanci FNOL mohou použít programy na prolomení hesel ke kontrole kvality hesel.

3.3 Používání internetu a elektronické pošty

3.3.1 FNOL si vyhrazuje právo:

a) Zakázat přístup k webovým stránkám s nepracovním a nevhodným obsahem.
b) Monitorovat přístupy uživatelů na webové stránky.
c) Automaticky blokovat elektronickou poštu obsahující nepracovní informace včetně příloh.
d) Regulovat dostupnost sítě internet jednotlivým uživatelům, korigovat jejích denní kapacitní limity přijatých a odeslaných dat z a do sítě internet.

3.3.2 Je zakázáno:

a) Odesílat poštovní zprávy (e-maily) s přílohami o velkém objemu dat, není-li to bezpodmínečně nutné pro splnění pracovního úkolu (zejména se jedná o zákaz příjmu hudby, obrázků apod.).
b) Obtěžovat uživatele odesíláním e-mailů obsahujících nevyžádaná data (spam) a data, která nemají pracovní charakter.

3.3.3 Správce prostředků ICT zajišťuje technickou podporu pouze služebnímu e-mailovému účtu (adrese), který uživateli zřídil.

3.4 Vzdálený přístup

Pro vzdálený přístup je nakoupen omezený počet licencí, které mají sloužit především ke konzultacím sloužícího personálu a odborného personálu mimo FNOL v akutních případech, kdy se jedná o ohrožení života pacienta nebo o získání časového náskoku. O vzdálený přístup s patřičným odůvodněním má právo žádat zaměstnanec FNOL svého nejvýše postaveného vedoucího pracoviště. V případě, že jeho důvody budou odpovídat výše uvedenému, vedoucí pracoviště zašle tento požadavek ke schválení náměstkovi informačních technologií. Na základě kladného rozhodnutí, nastaví OINF žadateli potřebná oprávnění. OINF současně vede přehled o přidělených právech vzdáleného přístupu.

3.5 Hlášení závad, hlášení požadavků na konzultace

3.5.1 Vyskytne-li se při provozu IS u jeho uživatele chyba, která brání uživateli v plnění pracovních povinností, je uživatel povinen nahlásit tuto chybu správci prostředků ICT.

3.5.2 K hlášení chyb a požadavků na konzultace musí použít aplikaci Call Centrum, pouze v případě její nedostupnosti využije tel. podporu na kl. 4516, která jeho požadavek nebo chybu zaeviduje. Neevidovaný požadavek nebude řešen.

3.6 Sankce

3.6.1 Uživatel zodpovídá za škody způsobené úmyslně či z nedbalosti.

3.6.2 Jakákoliv porušení směrnice je posuzováno jako závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci a následky tohoto jednání budou řešeny dle zákoníku práce.

3.7 Specifické odpovědnosti a pravomoci

3.7.1 Specifické odpovědnosti a pravomoci jsou uvedeny v textu.

3.8 Další odborní garanti

3.8.1 Tato ON nemá další odborné garanty.

4 SOUVISEJÍCÍ DOKUMENTY

4.1 Dokumenty vyšší úrovně

ČSN ISO/IEC 27001	Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky
ČSN ISO/IEC 27002	Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací

4.2 Dokumenty FNOL

Sm-I001	Provozování informačních technologií a informačních systémů
MP-I001-04	Řízení přístupu uživatelů k informačnímu systému

4.3 Vystavené dokumenty

Tato ON nevystavuje žádné dokumenty.

5 ZÁVĚREČNÁ USTANOVENÍ

5.1 Účinnost

5.1.1 Tato ON nabývá účinnosti dnem **11. 7. 2016.**

5.1.2 Dnem účinnosti se nenahrazuje žádná ON.

5.1.3 OG je povinen 1x za dva roky provést revizi ON. Pokud to stav vyžaduje, musí OG zajistit vypracování nového vydání ON nebo její změny. Záznam o provedené revizi provede správce dokumentace do formuláře Fm-G001-REV-001 „Záznam o revizi ON“.

Povinnost vypracování nové ON nebo změny nastává i v případě, že dojde k zásadním změnám, které se dotýkají obsahu ON.

5.1.4 Přechodná ustanovení nejsou stanovena.

5.2 Přílohy

Přílohy nejsou.