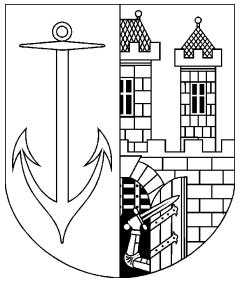

Městská část Praha 7 **tajemník ÚMČ Praha 7**

NAŘÍZENÍ

tajemníka č. 7 ze dne 13.12.2016
s účinností od 01.01.2017

Používání výpočetní techniky Úřadu MČ Praha 7

Schváleno usnesením Rady MČ Praha 7 č. 1262/16-R z jednání č. 80, ze dne 13.12.2016

OBSAH

I. Preambule

1. Tímto nařízením tajemníka se upravují pravidla provozu a bezpečnosti informačního systému Úřadu Městské části Praha 7 (dále jen „ÚMČ P7“). Informační systém úřadu (dále jen „IS“) je pro účely této směrnice definován jako soubor veškerého technického a programového vybavení určeného pro zpracování a ukládání informací v elektronické podobě. IS a informace v něm obsažené jsou majetkem a významným aktivem MČ Praha 7. Zodpovědnost za jeho ochranu mají všichni zaměstnanci ÚMČ P7.

2. Hlavním cílem tohoto nařízení je ochrana všech informací obsažených v IS před neautorizovanou změnou, únikem či zničením a zajištění jejich přesnosti, důvěrnosti a dostupnosti.

3. Toto nařízení je závazné pro všechny zaměstnance ÚMČ P7, pracovníky na detašovaných pracovištích, informačních centrech a všechny další uživatele, kterým bude umožněn přístup k výpočetní technice a informačním systémům.

4. Nedodržení tohoto nařízení může být posuzováno jako porušení pracovní kázně.

II. Organizační opatření

1. Základním dokumentem obsahujícím obecné bezpečnostní zásady používání výpočetní techniky v majetku ÚMČ P7 je toto nařízení tajemníka, které schvaluje Rada MČ Praha 7.

2. Za dodržování bezpečnostních pravidel a využívání IS k práci v rámci pracovní náplně v rámci jednotlivých odborů zodpovídají vedoucí odborů/oddělení.

3. Správa IS ÚMČ P7 spadá do kompetence Odboru informačních technologií (dále jen „IT“).

III. Kontakt na Odbor informačních technologií

1. Všichni uživatelé IS své požadavky a dotazy na IT uplatňují výhradně prostřednictvím aplikace HelpDesk. http://p7swap1/hesk/ Pokud aplikaci HelpDesk není možné použít (pc, monitor nebo připojení k síti nefunguje), pak je možné oznámit problém telefonicky nebo osobní návštěvou. IT řeší požadavky zaslané přes HelpDesk dle data a času přijetí, zároveň ale vyhodnocuje závažnost ostatních požadavků a dle potřeby je řeší prioritně.

IV. Zajištění bezpečnosti

1. Všichni zaměstnanci ÚMČ P7 jsou povinni chránit data a prostředky IS před neoprávněným přístupem nepovolaných osob, před úmyslnými nebo náhodnými změnami, destrukcí nebo únikem dat.

2. Kanceláře, ve kterých jsou umístěna pracoviště s PC a periferiemi, musí být v době nepřítomnosti zaměstnanců uzamčeny. Pracovník, který odchází z místnosti jako poslední, je povinen zamknout.

3. Všechny ostatní aktivní prvky sítě a rozvodné skříně jsou umístěny v uzamykatelných místnostech. Klíče od těchto místností mají pracovníci IT.

4. Pro síťové servery je zajištěno náhradní napájení, které umožní korektní ukončení provozu systémů a aplikací při výpadku elektřiny.

5. Zaměstnanci IT jsou povinni chránit veškeré údaje, které by mohli narušit bezpečnost provozu IS.

V. Pravidla pro používání počítačů

1. Počítače i jinou výpočetní techniku ÚMČ P7 je zakázáno používat pro soukromé účely s výjimkou zaměstnanců, kteří mají se zaměstnavatelem uzavřenou kvalifikační dohodu.

2. K počítačům je zakázáno připojovat a instalovat jakoukoliv soukromou výpočetní techniku či jiné zařízení neslužebního charakteru.

3. Počítače i jinou výpočetní techniku ÚMČ P7 je zakázáno demontovat nebo přemisťovat či odpojovat od datové sítě a napájení. V případě ohrožení zdraví a majetku však tento zákaz neplatí.

4. Technické prostředky IS (dále „HW“) jsou zabezpečena ochrannými kryty, jež je zakázáno snímat a provádět jakékoliv úpravy, montáže či demontáže HW komponent atd. Tyto činnosti jsou plně v kompetenci IT.

5. Je výslovně zakázáno používat soukromá velkokapacitní výměnná média (např. USB flash disky) pro ukládání pracovních dat.

6. Je zakázáno instalovat a používat (i spouštět z CD, USB apod.) jakýkoliv jiný software. V případě potřeby instalace nového SW se zaměstnanec obrátí na IT.

7. Je zakázáno měnit nastavení, vypínat nebo odinstalovat jakýkoliv software nainstalovaný na počítači. Uživatel je povinen dodržovat příslušné licenční ujednání SW instalovaného na jeho pracovní stanici.

8. Uživatelé IS jsou povinni nahlásit pracovníkům IT jakékoliv podezření na nesprávné fungování počítače nebo podezření na napadení počítačovým virem, případně jiné bezpečnostní riziko.

9. Uživatelé IS jsou povinni umožnit pracovníkům IT přístup ke svému počítači a na vyžádání s nimi spolupracovat.

10. Každý uživatel IS je osobně zodpovědný za všechny úkony provedené na počítači a v počítačové síti úřadu, které byly autorizovány jeho jménem a heslem.

11. Pracovníci IT mohou používat ke své práci vzdálený přístup přímo na pracovní plochu zaměstnanců, tam kde je nainstalována aplikace TeamViewer. Vždy na základě zaslaného požadavku přes HelpDesk. Bez vědomí uživatelů nesmí pracovníci IT připojení vzdáleného přístupu používat.

VI. Přenosné počítače (notebooky, tablety)

1. Přenosné počítače nesmějí být ponechány bez dozoru na nezabezpečeném místě. Uživatelé, kterým byl takový počítač přidělen, jsou zodpovědní za dostatečnou ochranu přenosného počítače při používání mimo budovu a chráněné prostředí počítačové sítě ÚMČ P7.

2. V případě krádeže je uživatel povinen tuto skutečnost neprodleně nahlásit svému nadřízenému a pracovníkům IT.

3. Uživatel musí průběžně zajišťovat aktualizaci antivirového programu a aplikaci bezpečnostních záplat operačního systému připojením notebooku k internetu na dostatečně dlouhou dobu nebo požádat o aktualizaci SW pracovníky IT.

4. Přihlášení do notebooku musí být chráněno dostatečně silným heslem (viz kapitola X. Používání hesel)

VII. Práce s tiskárnami

1. Je zakázáno používat tiskárny a podobná výstupní zařízení pro soukromé účely.

2. IT může v případě potřeby provoz tiskáren monitorovat (kdo tiskne, co tiskne).

3. Jsou-li tiskovým výstupem citlivé informace, je nutno chránit tyto výtisky tak, aby v době tisku nedošlo k úniku informací mimo ÚMČ P7.

4. Zabezpečení výstupů (tištěných či kopírovaných dokumentů) je možno realizovat:
   - zajištěním fyzické přítomnosti uživatele, příp. jím pověřené oprávněné osoby u daného zařízení před zahájením tisku;
   - ověřením, že v zařízení (tiskárně/kopírce), jeho okolí, ani v tiskových frontách nezůstaly dokumenty obsahující citlivé údaje;
   - nadbytečné nebo chybné výtisky je třeba příslušným způsobem skartovat.

5. Uživatelé jsou povinni hospodárně nakládat s prostředky ÚMČ P7, netisknout dokumenty zbytečně, jako např. tisk e-mailů, každoměsíční tisk aktualizovaného Bulletinu apod. K rychlému vyhledání kontaktu lze využít kombinaci kláves CTRL+F.

6. Jakoukoliv poruchu zařízení nahlásí uživatel pomocí HelpDesku na IT a nesnaží se závadu odstranit sám neodborným zásahem.

VIII. Nakládání s daty

1. Pod pojmem data se pro účely tohoto nařízení rozumí veškeré údaje a informace uložené v IS ÚMČ P7.

2. Každý uživatel je povinen se seznámit s platnými bezpečnostními směrnicemi o používání IS (příručkami, relevantními pracovními postupy a metodickými pokyny apod.), pravidly pro práci s nimi a dodržovat zde stanovená pravidla a nařízení.

3. Přístup k IS je dovolen pouze pracovníkům ÚMČ P7 a členům orgánů MČ Praha 7. Ostatním osobám není přístup povolen. Výjimku tvoří pouze zástupci dodavatelů informačních technologií, kteří mohou k IS přistupovat při instalacích a servisních zásazích a to vždy za účasti pracovníka IT, nebo dle dané servisní smlouvy.

4. Řízení přístupu k datům v IS je prováděno pomocí bezpečnostních mechanismů systémových nástrojů a aplikací. Cílem je identifikovat a autentizovat uživatele informací a přidělit mu taková oprávnění pro činnosti v systémech a aplikacích, která jsou nezbytná pro výkon jeho pracovních povinností.

5. Nastavení přístupových práv uživatele provádějí pracovníci IT na základě požadavků vedoucího příslušného odboru a na základě vstupního listu nového zaměstnance viz příloha č. 1. Žádný uživatel nemá přístup k datům, která nejsou relevantní k jeho funkčnímu zařazení. Kontrolu přístupových práv provádí IT nejméně jednou ročně. V případě, že uživatel zjistí, že má přístup tam, kam by přístup neměl mít, je povinen tuto skutečnost oznámit IT.

6. Veškerá data jsou ukládána na severy buď do databází, nebo na centrální datová úložiště do vyhrazených adresářů. Uživatelé jsou povinni na síťových discích udržovat pořádek a odmazávat již nepotřebné soubory.

7. **Lokální disky počítačů nejsou zálohovány.** V případě poruchy PC může dojít ke ztrátě dat (viz kapitola XII. Zálohování dat). Z toho důvodu je požadováno ukládání dat na síťová úložiště, která jsou pravidelně zálohována (disk Q – osobní soubory a disk X pro soubory, ke kterým mají mít přístup ostatní zaměstnanci odboru/úřadu). Podrobnosti viz příloha č. 3.

8. Na diskové prostory v rámci počítačové sítě nesmí být ukládána data soukromého charakteru.

9. Uživatelé IS jsou povinni zachovávat mlčenlivost o získaných informacích.

10. Uživatel nesmí v žádné formě zneužívat data ÚMČ P7 a poskytovat je třetím osobám. Za předávání dat mimo IS ÚMČ P7 vždy zodpovídá vedoucí příslušného odboru.

11. Každý uživatel IS je osobně odpovědný i za vytištěné dokumenty na svém stole. V případě, že se vzdálí, je povinen tyto dokumenty uschovat a zabránit tak možnému úniku citlivých informací. Každý uživatel je odpovědný za data uložená na přenosných nosičích (CD, DVD, flash disk, paměťové karty)

12. V případě vyřazování či předávání výpočetní techniky mimo ÚMČ P7 jsou zaměstnanci IT povinni nenávratně vymazat všechna data.

IX. Přidělování a rušení přístupu do IS

1. Při nástupu nového pracovníka je přístup do IS přidělen na základě tzv. vstupního listu nového zaměstnance, který je přílohou č. 1 tohoto nařízení. Vstupní list vystavuje personální oddělení a následně je doplňuje vedoucí odboru. Vedoucí odboru je zodpovědný za určení agend, do kterých má mít nový pracovník přístup.

2. V případě potřeby může vedoucí odboru požádat o přidělení (nebo odebrání) oprávnění do další agendy formou zaslání požadavku na HelpDesk.

3. Uživateli je správcem systému přiděleno jedinečné přihlašovací jméno a nastaveno výchozí heslo. Toto heslo je uživatel povinen změnit při prvním přihlášení do systému. Pravidla pro tvorbu hesla jsou definovány v kapitole X. Používání hesel.

4. Znepřístupnění uživatelského účtu při odchodu pracovníka (ukončení pracovního poměru) probíhá na základě výstupního listu zaměstnance, který je přílohou č. 2. Výstupní list vyplňuje vedoucí odboru, který zároveň stanoví způsob předání agendy. Vedoucí odboru je zodpovědný za předání výstupního listu zaměstnance IT nejpozději ke dni odchodu pracovníka. Účet je zneplatněn bezprostředně a to k datu uvedeném ve výstupním listu.

X. Používání hesel

1. Heslo je spolu s přihlašovacím jménem uživatele prvním vstupním bodem do IS. Z tohoto důvodu musí mít heslo určitou kvalitu, aby nebylo případným útočníkem snadno odhalitelné.

2. Požadavky na kvalitu hesla jsou:
   - Minimální délka hesla je 8 znaků. Je však upřednostňováno heslo delší.
   - Heslo musí obsahovat alespoň jedno malé písmeno (a-z), alespoň jedno velké písmeno (A-Z), alespoň jednu číslici (0-9) a alespoň jeden speciální znak (_ + - !)
   - Je zakázáno používání známých jmen, osobních údajů a jiných lehce odhalitelných hesel (jako je rodné číslo, jména členů rodiny, názvy předmětů v blízkosti počítače, běžných jednoduchých slov umožňujících tzv. slovníkový útok ap.).
   - Z důvodu nové bezpečnostní politiky je nastavena platnost hesla na 180 dní, poté je nutné si heslo opět změnit. Hesla se nesmí opakovat, přílišná podobnost předchozímu heslu není umožněna.
   - Heslo lze změnit stisknutím kláves Ctrl+Alt+Delete -> změnit heslo.

3. Uživatelé jsou povinni dodržovat zásadu privátnosti hesla, tj. nesdělování hesla kolegům a nezapisování na lehce přístupná místa (zápisník, okraj monitoru, kalendář, spodní strana klávesnice apod.). V případě potřeby lze poskytnout heslo svému určenému zástupci.

XI. Zálohování dat

1. Hlavním nástrojem na ochranu dat je systém zálohování. Zálohování dat, včetně programových souborů vybraných aplikací probíhá každý pracovní den v nočních hodinách.

2. Zálohovány jsou servery a centrální datové úložiště (síťové disky). **Lokální disky počítačů zálohovány nejsou.** Uživatelé mají zakázáno ukládat pracovní soubory na lokální disk počítače, kde hrozí jejich ztráta v případě poruchy či jiné nenadálé události. (např. výpadek el. proudu, poškození disku, zavirování apod.).

XII. Antivirová ochrana

1. Na počítačích uživatelů, připojených do sítě ÚMČ P7, je nainstalován antivirový program, který automaticky vykonává antivirovou kontrolu počítače v reálném čase (bez nutnosti zásahu uživatele) a plánované skenování počítače na případný výskyt škodlivého kódu.

2. V případě podezření na e-mail se zavirovanou přílohu, kdy příloha je nejčastěji v podobě *.zip souboru, tvar e-mailové adresy je „podivný“ (jeho tvar nedává smysl), neznáte odesílatele nebo takový e-mail neočekáváte, měli byste být obezřetní. Soubory *.zip od neznámého odesílatele neotvírejte. S prověřením souborů se obraťte na IT.

3. Uživatelé nesmí jakkoliv zasahovat do konfigurace antivirového programu, vypínat jej nebo jinak bránit jeho činnosti.

4. Veškerá CD, DVD, USB flash disky apod. musí být před jejich použitím nejprve prověřeny antivirovým programem. Jak na to: Tento počítač -> pravé tlačítko myši na umístění USB flash disku nebo jiného přenosného zařízení -> scan with Sophos nebo scan with AVG.

5. V případě virové nákazy nebo podezření na ni musí uživatel tuto skutečnost neprodleně nahlásit IT.

XIII. Používání internetu

1. Mezi základní komunikační prostředky, provozované pomocí výpočetní techniky, jsou v IS ÚMČ Praha 7 elektronická pošta a Internet. Nesprávné používání či zneužívání elektronické pošty nebo Internetu může vážným způsobem omezit nebo ohrozit bezpečnost IS.

2. **Uživatelům je zakázáno:**
   - používat internet k jiným než pracovním účelům;
   - poslouchat internetová rádia, pouštět online filmy a zatěžovat tak zbytečně počítačovou síť a omezovat tak rychlost internetu;
   - navštěvovat internetové stránky s nevhodným obsahem např. pornografické stránky, stránky zobrazující násilí, podněcující k rasismu; stránky, jejichž obsah je v rozporu s platnými zákony, herní portály, online zábavné hry a sázkové portály, kasina apod.;
   - stahovat (kopírovat) jakákoliv data neslužebního charakteru;
   - používat sociální sítě a veřejné komunikační kanály, kromě případu, kdy používání sociálních sítí vyplývá z pracovní náplně (např. oddělení komunikace).

3. Připojení k internetu je realizováno prostřednictvím privátní sítě (MePNet), kterou spravuje Magistrát hl. m. Prahy.

4. Připojení k Internetu je realizováno a spravováno prostřednictvím systémového nástroje (tzv. firewall), který umožňuje odfiltrovat nebezpečnou komunikaci.

5. Internetový provoz ÚMČ P7 může být monitorován za účelem udržení stanovené úrovně bezpečnosti, technické údržby, řešení technických problémů apod.

6. Přístup k Internetu mají umožněn všichni uživatelé IS ÚMČ P7 a to v souladu se základními pravidly a zásadami pro používání Internetu.

XIV. Používání elektronické pošty

1. Pomocí elektronické pošty nesmí být posílána jakákoliv data a přílohy neslužebního charakteru. Ke služebním účelům je zakázáno používat poštovní schránky zřízené u externích poskytovatelů.

2. Každý uživatel je povinen dodržovat pravidla údržby své e-mailové schránky:
   - pravidelně mazat staré (nepotřebné) e-maily;
   - pravidelně archivovat e-maily, které nejsou aktuální, ale je nutné je uchovat;
   - pravidelně odstraňovat e-maily přesouvané do složky „Odstraněná pošta“.

3. Zodpovědnost za vyřízení e-mailové korespondence nesou jednotliví uživatelé – vlastníci poštovní schránky (mailboxu).

4. Veškerá příchozí pošta je filtrována antivirovým a antispamovým systémem. Každý uživatel má možnost se zaregistrovat k službě doručování zadrženého spamu prostřednictvím žádosti na IT.

5. Uživatelé mohou využít pro elektronickou komunikaci adresu http://posta.praha7.cz, která je dostupná odkudkoli z internetu, tedy i mimo úřad.

XV. Provoz sítě

1. Provoz sítě je garantován v pracovní době s výjimkou akcí MČ Praha 7. Čas mimo pracovní dobu je vyhrazen na údržbu a další servisní činnosti.

2. Před ohlášeným vypnutím el. proudu je uživatel povinen předem ukončit práci na PC a vypnout jej. Při mimořádných nečekaných výpadcích el. proudu je nutné PC následně vypnout a s jeho zapnutím počkat 5 minut po opětovném zapnutí el. proudu z důvodu možného dalšího výpadku nebo kolísání napětí.

XVI. Licenční politika

1. Veškerý software v IS ÚMČ P7 musí být používán v souladu s platnými právními předpisy a příslušnými licenčními ujednáními. Pracovník nesmí jakýmkoliv způsobem dále šířit (a to ani bezúplatně) žádný počítačový program, který je součástí IS ÚMČ P7. Instalovaný software je evidován v evidenci IT.

2. Veškeré instalace a konfigurace počítačových programů provádí pouze pracovník IT.

3. Zaměstnanec nesmí používat, či poskytnout jiným uživatelům, jakékoliv neoprávněně získané klíče, sériová čísla či jiné technické prostředky sloužící k zajištění informační bezpečnosti a ochraně počítačových programů.

4. Zaměstnanec nesmí odstranit jakékoliv informace, označení či zařízení identifikující nositele či vykonavatele autorských práv k počítačovým programům, autora či jinou oprávněnou osobu.

5. Instalace a užívání nelegálního nebo neschváleného SW je považováno za hrubé porušení pracovní kázně. Za případné trestněprávní důsledky, které vyplynou z užívání nelegálního SW, nese plnou odpovědnost uživatel.

6. Nejméně 1x za půl roku je prováděn audit nainstalovaného SW a kontrola licencí.

XVII. Elektronický podpis

1. Žádost o vyřízení certifikátu pro vytváření elektronických podpisů podává příslušný vedoucí odboru formou interního sdělení na IT. V žádosti musí být uveden důvod a účel používání.

2. Žádost o vyřízení certifikátu pro vytváření elektronických podpisů lze podat až po uplynutí zkušební doby.

3. Každý pracovník, který je vybaven certifikátem pro vytváření elektronického podpisu, je povinen tento certifikát chránit proti ztrátě či zneužití. V případě podezření na zneužití certifikátu je pracovník povinen toto nahlásit na IT, který certifikát zneplatní.

4. Při rozvázání pracovního poměru se certifikát zneplatní. Zneplatnění certifikátu zajistí IT na základě vyplněného Výstupního listu dle přílohy č. 2 tohoto nařízení.

XVIII. Pravidla pro opuštění pracoviště

1. Uživatelé jsou povinni zabezpečit kancelář při jejím opuštění.

2. Každý zaměstnanec osobně zodpovídá za to, že na pracovišti nebudou ponechána:
   - volně přístupná data služebního charakteru;
   - žádná data, software, hardware, přenosná média či další věci, které nemají souvislost s jeho prací, nebyla mu přidělena z důvodu jeho práce, nejsou zkušební či jiné povahy související s jeho prací a/nebo nejsou legálně obhajitelná.

3. V případě krátkodobého opuštění kanceláře je povinností každého uživatele uzamknout PC (stiskem kláves Ctrl+Alt+Delete a následným stiskem klávesy Enter, případně stiskem kláves „Windows“ + L, nebo odhlášením ze systému).

XIX. Závěrečné ustanovení

Toto nařízení nabývá účinnosti dne 01.01.2017.

Příloha č. 1

VSTUPNÍ LIST NOVÉHO ZAMĚSTNANCE

Jméno a příjmení	
Osobní číslo	
Pracovní zařazení	
Odbor/útvar	
Datum nástupu	
POŽADAVKY NA ZAJIŠTĚNÍ PRACOVNÍCH PODMÍNEK NOVÉHO ZAMĚSTNANCE	
Informatika	
Pracovní pozice	**Po kterém zaměstnanci nastupuje/nová pozice**
GINIS + název modulu (ano - modul UCR,SML atd.)	
přístup do základních registrů a rozsah oprávnění ROB, ROS, RUIAN, RPP (certifikáty se vystavují až po zkušební době)	
e - spis/funkční místo (ano - například ORZ_REF4)	
přístup do Codexis (ano/ne)	
přístup do jiné aplikace (OKnouze, ENO, EVI, Misys atd…)	
AIP safe + členství ve skupinách (ano - například DMS.Uzivatel)	
notebook (ano/ne)	
Další vybavení (například scanner…)	
Provozní oddělení KST	
mobilní telefon	ano/ne
aktivace	ano/ne
datové služby	ano/ne
ochranné pracovní prostředky	
školení řidičů referentských vozidel	ano/ne
Personalistika/vzdělávání	
vstupní školení	
zkoušky odborné způsobilosti	
jiné školení	
Jiné požadavky - specifikovat	
Praha dne:	
Navrhl:	Schválil: Ing. Radomír Špok, tajemník ÚMČ P7

Příloha č. 2

Výstupní list
(pro zrušení přístupu do IS ÚMČ P7)

Vyplní vedoucí odboru: *(a dále zašle na odbor informatiky)*

Příjmení a jméno:

Odbor:

Oddělení:

Ukončení pracovního poměru ke dni:

Pokyny pro předávání elektronických dat:

Poštovní schránku: ☐ zrušit
☐ přesměrovat na 1 měsíc: komu a po té zrušit
☐ překopírovat zprávy: komu

Dokumenty ☐ smazat nenávratně
☐ překopírovat: komu
☐ archivovat a předat vedoucímu odboru

Písemnosti ve spisové službě:
☐ předat: komu
☐ ponechat na funkčním místě a přidat zastupování komu:

Písemnosti v AIP-SAFE:
☐ předat: komu
☐ ponechat na funkčním místě a přidat zastupování komu:

Kvalifikovaný zaměstnanecký certifikát ANO – NE Datum zneplatnění:

Příloha č. 3

Popis datového úložiště (disk X s názvem DATA MUP7)

ODBOR - Úložiště pro data odboru. Přístup mají jen uživatelé patřící do odboru.

SDILENE - Výměnné úložiště mezi odbory/uživateli. Všichni vidí do složek a mohou je číst.

SKUPINY - Úložiště pro specifické skupiny uživatelů. Přístup mají jen vybraní uživatelé.

Uložiště je chráněné proti selhání (pole raid5) a jeho obsah je časově zálohován (každý den, uchováván jeden pracovní týden zpět).

Viditelné jsou pouze složky, kam máte přístup (alespoň čtení, nebo zápis). Přístupy a struktura se budou dále upřesňovat. Případné požadavky na přístup a další složky formou HelpDesku.

Popis datového úložiště (disk Q s názvem Personal Disk)
Toto úložiště slouží k uchovávání dokumentů xls, pdf, doc a jiných, na kterých pracujete. Síťový disk je pravidelně zálohován. Lokální disk zálohován není, tzn., že při poruše disku je nemožné nebo velmi obtížné data obnovit.