INFORMATIKAI

SZABÁLYZAT

RUDABÁNYA VÁROS ÖNKORMÁNYZATA

POLGÁRMESTERI HIVATAL

5/2010. jegyzői rendelkezés

Rudabánya Önkormányzatának a Számítástechnikai Védelmi Szabályzatát (továbbiakban: SZVSZ) a következők szerint határozom meg:

1. Számítástechnikai Védelmi Szabályzat célja

A Rudabánya Polgármesteri Hivatal adatvédelmi besorolása alap biztonsági fokozat.

Indoklás

Állami illetve Szolgálati titkot képező adatok számítógépes folyamat közbeiktatásával történő feldolgozása nincs, illetve számítógépes feldolgozás eredménye után minősített adatok nem keletkeznek.

A hivatalban munkaviszonyban, vagy munkavégzésre irányuló jogviszonyban álló természetes személyekről számítógépes nyilvántartást jegyzői engedély alapján végeznek.

Az SZVSZ alapvető célja, hogy a számítástechnikai alkalmazása során biztosítsa az hivatalnál az alábbiakat:

- titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozás és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre való csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- munkaállomásokon (USER) lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését,
- a számítógépes rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit,
- a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen SZVSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét. Szabályozza a számítástechnikai eszközök használatának és a szoftverkészítés feladatának adatvédelmi, biztonsági szabályait.

2. A szabályzat hatálya

Az SZVSZ személyi hatálya az intézmény (hivatal) valamennyi fő- és másodállású, mellék-, és részfoglalkozású dolgozójára, illetve a számítástechnikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed valamint minden számítástechnikai folyamattal előállított, tárolt vagy

feldolgozott adatok teljes körére, felmerülésük és feldolgozásuk helyétől és idejétől, valamint az adathordozó fizikai megjelenési formájától függetlenül.

Tárgyi hatálya kiterjed

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül (elsődleges adathordozók a bizonylatok, különböző tablók stb.)
- szervezet tulajdonában lévő, illetve az általa bérelt valamennyi számítástechnikai berendezésre, valamint a gépek műszaki dokumentációira is,
- a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer- és felhasználói programokra
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

3. A szabályzathoz kapcsolódó szabályozások

A rendelet értelmében, ha a szervezet – alap – biztonsági fokozatba tartozik, akkor technikai technológiai bizonylati fegyelem betartását a dokumentációk meglétét az egységes eljárások előírásait és a hatékony működését biztosító feltételeket kell rögzíteni.

Ha a hivatal minősített feldolgozásokat végez, akkor rendelkeznie kell az alábbiakról:

- adatállomány nyilvántartásba vétele,
- a bizonylatok áramlási útja,
- alkalmazandó védelmi módszerek és eszközök,
- adatok tárolásának és kibocsátásának módja
- hibás és fölöslegessé vált adatok selejtezési és megsemmisítési rendje,
- hozzáférési jogosultság,
- ellenőrzési jogosultságok és kötelezettségek.

Az SZVSZ-t az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Ügyviteli Szabályzat,

4. Védelmet igénylő adatok, eszközök köre

A védelem tárgya

- az alkalmazott hardver eszközök és azok működési biztonsági,
- a számítástechnikai eszközök üzemeltetéséhez szükséges okmányok és
- dokumentációk,
- az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága,
- személyhez fűződő és vagyoni jogok (jogtalan belső és minden külső fél),

- az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.

A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási jogi, ügyrendi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik illetve biztosítják.

5. Az SZVSZ alkalmazásának módja

Az SZVSZ-t oktatás keretében meg kell ismertetni a számítástechnikai alkalmazás folyamatában résztvevő dolgozókkal

A titkos adatokkal kapcsolatos tudnivalókról csak azokat a dolgozókat kell kioktatni, akiknek a kérdéses adatokba, információkba betekintési joguk van. Az oktatás megszervezése és az oktatási anyag összeállítása az adatvédelmi felelős feladata.

A munkaköri leírásokat ki kell egészíteni az adott munkakörre vonatkozó adatvédelmi feladatokat kijelölő és a betekintési jogot meghatározó záradékkal.

Az SZVSZ karbantartása

Az SZVSZ-t a számítástechnikában – valamint a hivatalnál – a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

Az SZVSZ-ben bekövetkezett változásokról az arra illetékes dolgozókat tájékoztatni kell.

6. Számítástechnikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas számítógépek és egyéb hardver berendezések fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel, a veszélyhelyzetek elháríthatók legyenek.

Elemi csapások, környezeti ártalmak

1. Elemi csapás: földrengés, árvíz, (a keletkezett kár csak a biztosító kártérítésével ellensúlyozható).
2. Környezeti kár:
    - légszennyezettség, nagy teljesítményű elektromágneses és optikai térerő,
    - fokozott tűz- és robbanásveszély

    (Ezeket a körülményeket a létesítmény építésénél, illetve az épület használatba vétele előtt figyelembe kell venni).
3. Közüzemi szolgáltatásba bekövetkező zavarok
    - feszültség-kimaradás
    - feszültségingadozás
    - vízhiány

Emberi tényezőkre visszavezethető veszélyek

Szándékos károkozás

- behatolás a számítástechnikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz)
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal vírusfertőzött szoftver behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása (hibás működést, vagy az eszközök meghibásodását idézheti elő),
- a szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása (veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz).

7. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adat-előkészítés, az ellenőrzési szempontok hiányos betartása.

A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- program tesztelés elhagyása (működés hiányos ellenőrzése).

A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

8. A számítástechnikai eszközök környezetének védelme

Általános védelmi előírások

A hardware és software eszközök fizikai környezete feleljen meg az érvényes munkavédelmi és ergonómiai előírásoknak, valamint a hardware és adattároló eszközöket gyártók üzemszerű működést garantáló előírásainak.

A számítástechnikai egységek tűzvédelmére vonatkozó konkrét szabályokat a hivatal tűzvédelmi utasítása, valamint szerződés alapján a biztosító által meghatározott feltételek tartalmazzák.

Vagyonvédelmi előírások

- a hivatal külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- az irodákba való be- és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak az adatfeldolgozó helyeken, vagy a hivatalos helységekben.
- munkaidőn túl a hivatalban csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek nem olvashassák el,
- a hivatalba, adatfeldolgozó helyre történő illetéktelen behatolás tényét a gazdálkodó szervezet vezetőjének azonnal jelenteni kell,
- az irodahelyiségben elhelyezett számítástechnikai eszközöket csak a kijelölt dolgozók használhatják,
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni (erről nyilvántartást kell vezetni),
- a használni kívánt adathordozót (floppy disc-et) a tárolásra kijelölt helyről kell kivenni és oda kell vissza is helyezni.
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót más intézménynek átadni csak engedéllyel szabad (átadást csak a vezető engedélyezheti),
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Tűzvédelem

A hivatal illetve az egyéb kiszolgáló helyiség a "D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A tűzvédelem feladatait, sajátos előírásokat a gépterem (számítógépes szoba)

"Tűzvédelmi utasítás" tartalmazza (ez a gazdálkodó szervezet tűzvédelmi utasításának részét képezi).

Ebben meg kell határozni az alábbiakat:

- tűzvédelmi eljárásokat,
- tűzmentési eljárásokat,
- menekülési útvonalakat,
- fontosabb mentési eljárásokat.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a számítógépterem és az adatállomány-tároló helység között.

A nagy fontosságú pl. törzs-adatállományokat 2 pld.-ban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

Ezen adatállományok kijelölése a rendszergazda feladata. A gépteremben vagy irodákban csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. leporellót).

9. A számítástechnikai alkalmazásánál felhasználható védelmi eszközök és módszerek

A gépterem és a számítógépet befogadó irodahelyiség védelme

Elemi csapás vagy a gépterem illetve irodahelyiség részleges vagy teljes károsodásakor a lehetséges intézni valókat az "**Informatikai katasztrófa-terv**" tartalmazza:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. A karbantartási munkát tervezetten, körültekintően és gondosan kell elvégezni.

A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- tapasztalatokat,
- hardver tesztek által feltárt hibákat.

A számítástechnikai alkalmazás folyamatának védelme

Az adatrögzítés védelme:

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- csak tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses és optikai adathordozókat csak e célra kialakított és megfelelő tárlóhelyeken szabad tartani,
- adatrögzítés szoftver védelme (a programokat ellenőrző funkciókkal kell ellátni,

ellenőrző számok, kontrollösszegek használatát biztosítani kell).

Biztosítani kell a rögzített tételek visszakeresésének és javításának lehetőségét.

Hozzáférési lehetőség:

- a bejelentkezési azonosítók használatával lehet szabályozni, hogy ki milyen szinten férhet hozzá (Alapelv: a tárolt adatokhoz csak illetékes szervezeti egységek személyei férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyan az a személy nem végezheti.

Adathordozók védelme

Az adathordozók logikai védelemét az operációs rendszer és az ehhez tartozó ellenőrző, file kezelő rutinok alkalmazásával lehet biztosítani. A számítástechnikai berendezések üzemeltetéséért a rendszergazda köteles gondoskodni a feldolgozások igényeink megfelelő mágneses és optikai adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

Adathordozók tárolása

Az adathordozók tárolására a géptermen kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani. Mágneses és optikai adathordozót a részlegből ki illetve oda bevinni csak az üzemeltetésért felelő vezető engedélye alapján lehet.

Nyilvántartás

A mágneses és optikai adathordozókról egyedi azonosítóként nyilvántartást kell vezetni. Az azonosító adaton kívül a felírás és megőrzés dátumát, védettség tényét, jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell tartalmaznia. A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.

Megőrzés

A megőrzés idejét, ha másképp nincs rendelkezés, az üzemeltető és a megrendelő közösen határozzák meg. A megőrzési idők nyilvántartásáért és ezek betartatásáért az adatállományok nyilvántartását végző személy a felelős.

Karbantartás

Az adathordozókat félévenként tisztítani kell és ellenőrizni a mágneses és optikai adathordozók állapotát, elöregedését.

Selejtezés, sokszorosítás, másolás

Olyan mágneses és optikai adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Tehát:

- fizikailag sérült javíthatatlan,
- gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott),

- mágneslemeznél, ha a kapacitás a névleges érték 75%-ánál kevesebb,
- véglegesen elhasználódott (leporelló).

Az alkalmatlan mágneslemezeket fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó mágneses és optikai adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Selejtezési Szabályzatnak és a szervezet iratkezelési szabályzatának megfelelően kell lefolytatni.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. (Az üzemi másolás nem minősül másolásnak). Biztonsági illetve archív adatállomány előállítása másolásnak számit.

Leltározás

A mágneses és optikai adathordozókat a Leltározási Szabályzat-nak megfelelően kell leltározni.

File-ok védelme

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó mágneses és optikai lemezekről másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

10. Szoftver védelem

Rendszerszoftver védelem

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést biztosítani kell, az illetéktelen próbálkozást ki kell zárni.

Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

A feldolgozás biztonságának megvalósításának megvalósításához naprakész állapotban kell tartani a program dokumentációit.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója,
- a program készítőjének neve,
- a feldolgozási rendszer megnevezése.

Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni az adatokról, programokról.

Információk védelme az adat-feldolgozási rendszer egyes szakaszaiban

a) Fejlesztés, tervezés fázisa

Fontos a tartalmilag helyes adatok előállítása, a rendszer biztonságos üzemeltetése és a veszélyek elleni védekezés Az eredmény megjelenítése (leporelló, képernyő) tervezésekor ügyelni kell a szükséges és elégséges információmennyiség biztosításáról. Gondoskodni kell az eredményadatok ellenőrzési módszereinek kidolgozásáról.

A bemeneti információk és adathordozók tervezésekor fokozottan kell ügyelni az ellenőrzési szempontok beépítésére.

b) Szervezési fázis

A felhasználó igénye szerint minősíteni kell az előkészítendő rendszert. A minősítést a rendszer szervezési dokumentációjában rögzíteni kell. El kell készíteni az adatok kimentésének és a kiindulási adatok meghatározott idejű megőrzésének előírását.

c) Programozási fázis

- törekedni kell az áttekinthető programok készítésére,
- kísérő információkkal kell ellátni a programokat, így később szükségessé váló módosítások nagyobb biztonsággal és kevesebb ráfordítással végezhetők el.
- a programstruktúrát modulárisan kell felépíteni,
- a modulok Inputját-outputját egyértelműen definiálni kell,
- biztosítani kell, hogy a tesztelés teljes körű legyen.

Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezettség dokumentálásának.

A dokumentációról nyilvántartást kell vezetni, s ennek az alábbiakat kell tartalmaznia:

- rendszer megnevezése,
- dokumentáció típusa,
- a rendszer adatvédelmi minősítése,
- a kidolgozók névsora,
- példányszám és tárolás helye,
- az átadás ideje,
- módosítások megnevezése és ideje.

11. A központi számítógép(ek) és a hálózat munkaállomásainak működés biztonsága

Központi gépek (Server)

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól naponta biztonsági mentést kell készíteni. A mentés felülírással készül, így mindig 1 nappal korábbi

állapotú adat-visszaállítást kell lehetővé tenni. Az alkalmazott hálózati operációs rendszer pl. NOVELL adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet. Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell. Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad. Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

A hivatal számítógépeiről programot ill. adatállományt másolni a jogos belső felhasználói igények kielégítésén kívül nem szabad.

Olyan floppy lemezeket, melyeken a formattálás után az operációs rendszer rossz szektorokat mutat ki, TILOS felhasználni.

A hálózati vezeték (KOAX KÁBEL, UTP) és egyéb csatoló elemet rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

A számítástechnikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A Számítástechnikai Védelmi Szabályzat 2010. január 2.napjával lép hatályba.

Rudabánya, 2010. január 2.

Dr. Sallai Árpád
Címzetes főjegyző

1. sz. melléklet

Az adatfeldolgozás rendje

a) Az adatrögzítő helyiségében az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:
   - hivatal vezetője,
   - egyéb vezetők,
   - szervezők, programozók, műszaki szakemberek.

   Más személyek benntartózkodását csak a hivatal vezetője engedélyezheti.

b) Üzemeltetés alatt az ajtókat állandóan becsukva, üzemidőn kívül pedig zárva kell tartani és a kulcsokat le kell adni.

   A gépterem, irodák kulcsát csak a hivatalvezetője által összeállított külön listán szereplő személyek kaphatják meg.

   Munkaidőn kívül idegen személy csak a hivatal vezetőjének (távollétében helyettesének) engedélyével tartózkodhat a gépteremben, irodákban.

   A gépterem és az adatrögzítő helyiség romtalanításáért a kijelölt gépkezelő a felelős. (Kivéve Okmányiroda és a központi server)

c) A gépteremben, irodákban az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni. A géptermi rend megtartásáért, a biztonságos műszaki üzemeltetésért a megbízott rendszergazda felelős.

d) A gépterembe ételt, italt bevinni és ott elfogyasztani **TILOS**!

e) **SZIGORÚAN TILOS** a gépteremben, irodákban égő cigarettával belépni, illetve ott dohányozni!

f) A gépterem takarítását csak az arra előzőleg kioktatott személyek végezhetik.

g) A berendezések belsejébe nyúlni **TILOS**! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak az informatikus vagy rendszergazda végezheti. Ez alól csak a szervizek szakemberei kivételek.

h) A számítógépeket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.

i) A gépteremben, irodákban elhelyezett adathordozókhoz a gépkezelőn (adatrögzítő) kívül, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.

j) Adathordozókat, mágneslemezeket, mágnes-kazettákat és leporellókat csak a gépkezelő engedélyével lehet kihozni, illetve bevinni a gépterembe, irodába.

k) Az elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet!

l) A gépteremben, irodákban elhelyezett jelzőberendezések (klíma, tűz- és betörés jelző) műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak és bármilyen rendellenességet azonnal jelenteni kell a működésükért felelős megbízottaknak.

m) A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

A fenti rendelkezések megsértése esetén fegyelmi felelősségre vonás kezdeményezhető.

Rudabánya, 2010. január 2.

dr.Sallai Árpád
Címzetes főjegyző

2. sz. melléklet

Adathordozók nyilvántartása

Az adatok nyilvántartási rendje

A nyilvántartás vezetése minden géptermi dolgozó számára kötelező a munkaköri leírásban meghatározottak szerint.

Az adatok mentési rendje

a) Napi mentések

Kötelező – a hivatal dolgozói számára munkaköri feladatként meghatározott – tevékenység az állományok napi mentése. A napi mentések megőrzési ideje: 5 nap (generációs mentés esetén).

b) Havi rendszeres archiválások

A hivatal havi munkatervében meghatározott időpontokban el kell végezni az állományok biztonsági mentését.

c) Rendkívüli archiválások

Minden olyan esetben – rendszergazda – közreműködésével - végre kell hajtani a futtatás megkezdése előtt, amikor az adatállományok reprodukálása ezt megköveteli.

Megőrzési idő: esetileg meghatározandó.

d) Éves rendszerességű archiválások

Végrehajtása kötelező a rendszerek évváltási metodikájának megfelelő időpontokban. A mentés tartalmazza az éves aktív állományok összességét.

Megőrzési idő: 5 év.

Rudabánya, 2010. január 2.

dr.Sallai Árpád
Címzetes főjegyző

3. sz. melléklet

Tűzvédelmi utasítás

A gépterem, valamint annak közvetlen kiszolgáló helyiségei "D" tűzvédelmi osztályba tartoznak, mely mérsékelten tűzveszélyes üzemet jelent.

1) A gazdálkodó szervezet azon helyiségeiben, ahol számítástechnikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os csak halonnal oltó tűzoltó készüléket kell elhelyezni. Nagyobb tűzoltó készüléket 4-nél több számítógép esetén kell használni.

2) Azokba a helyiségekben, ahol 1-nél több számítógéppel dolgoznak, az ott dolgozó munkatársak közül egy-egy tűzvédelmi megbízottat kell kijelölni.

   A kijelölt megbízottnak a tűzvédelmi utasításba előírt gyakorisággal tűzvédelmi vizsgát kell tenni.

3) A számítógép elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi megbízott tudtával, illetve engedélyével szabad végezni.

4) Tűzvédelmi és tűzmentesítési eljárásokon túl a menekülő utakat is meg kell határozni a szervezet vezetőjének, amelyet mindig szabadon kell hagyni.

5) Létfontosságú adatállományokról 2 pld-t mágneses és/vagy optikai adathordozón kell elhelyezni, és a két példányt elkülönítetten kell tárolni, tűzbiztos páncélszekrényben.

6) A számítógépteremben, irodákban gyúlékony anyagot csak a napi munkavégzéshez szükséges mennyiségben szabad tárolni (pl. leporelló).

Rudabánya, 2010. január 2.

dr.Sallai Árpád
Címzetes főjegyző

Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést biztosítani kell, az illetéktelen próbálkozást ki kell zárni.

Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

A feldolgozás biztonságának megvalósításának megvalósításához naprakész állapotban kell tartani a program dokumentációit.

11. A központi számítógép(ek) és a hálózat munkaállomásainak működés biztonsága

Központi gépek (Server)

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól naponta biztonsági mentést kell készíteni. A mentés felülírással készül, így mindig 1 nappal korábbi állapotú adat-visszaállítást kell lehetővé tenni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet. Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell. Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad. Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

A hivatal számítógépeiről programot ill. adatállományt másolni a jogos belső felhasználói igények kielégítésén kívül nem szabad.

Olyan floppy lemezeket, melyeken a formattálás után az operációs rendszer rossz szektorokat mutat ki, TILOS felhasználni.

A hálózati vezeték (KOAX KÁBEL, UTP) és egyéb csatoló elemet rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

A számítástechnikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A Számítástechnikai Védelmi Szabályzat 2010. január 2.napjával lép hatályba.

Rudabánya, 2010. január 2.

Rudabányai Közös Önkormányzati Hivatal Címzetes Főjegyző

dr.Sallai Árpád
Címzetes főjegyző

1. sz. melléklet

Az adatfeldolgozás rendje

a) A számítógépeket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.

b) A berendezések belsejébe nyúlni **TILOS**! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak az informatikus vagy rendszergazda végezheti. Ez alól csak a szervizek szakemberei kivételek.

c) Az elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet!

d) Irodákban elhelyezett jelzőberendezések (klíma, tűz- és betörés jelző) műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak és bármilyen rendellenességet azonnal jelenteni kell a működésükért felelős megbízottaknak.

e) A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

A fenti rendelkezések megsértése esetén fegyelmi felelősségre vonás kezdeményezhető.

Rudabánya, 2010. január 2.

Rudabányai Közös Önkormányzati Hivatal Címzetes Főjegyző

dr.Sallai Árpád
Címzetes főjegyző

2. sz. melléklet

ADATMENTÉSEK

a) Napi mentések

Kötelező – a hivatal dolgozói számára munkaköri feladatként meghatározott – tevékenység az állományok napi mentése. A napi mentések megőrzési ideje: 5 nap (generációs mentés esetén).

b) Havi rendszeres archiválások

A hivatal havi munkatervében meghatározott időpontokban el kell végezni az állományok biztonsági mentését.

c) Rendkívüli archiválások

Minden olyan esetben – rendszergazda – közreműködésével - végre kell hajtani a futtatás megkezdése előtt, amikor az adatállományok reprodukálása ezt megköveteli.

Megőrzési idő: esetileg meghatározandó.

d) Éves archiválások

Végrehajtása kötelező a rendszerek évváltási metodikájának megfelelő időpontokban. A mentés tartalmazza az éves aktív állományok összességét.

Megőrzési idő: 5 év.

Az adatok mentéséért felelős személy: Dobosi István Informatikus.

Rudabánya, 2010. január 2.

dr.Sallai Árpád
Címzetes főjegyző

3. sz. melléklet

Tűzvédelmi utasítás

a Polgármesteri Hivatal irodái "D" tűzvédelmi osztályba tartoznak, mely mérsékelten tűzveszélyes üzemet jelent.

1) A számítógép elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi megbízott tudtával, illetve engedélyével szabad végezni.

2) Tűzvédelmi és tűzmentesítési eljárásokon túl a menekülő utakat is meg kell határozni a szervezet vezetőjének, amelyet mindig szabadon kell hagyni.

3) Létfontosságú adatállományokról 2 pld-t mágneses és/vagy optikai adathordozón kell elhelyezni, és a két példányt elkülönítetten kell tárolni, tűzbiztos páncélszekrényben.

4) Az irodákban gyúlékony anyagot csak a napi munkavégzéshez szükséges mennyiségben szabad tárolni (pl. leporelló).

Rudabánya, 2010. január 2.

Rudabányai Közös Önkormányzati Hivatal Címzetes Főjegyző

dr.Sallai Árpád
Címzetes főjegyző