

Tét Város Polgármesteri Hivatal



INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Tét Város Önkormányzat Képviselő-testülete elfogadta a
188/2010. (XII. 22.) Képviselő-testületi határozattal.

jóváhagyta:

.....
Dr. Kukorelli László
polgármester

.....
Bereczkiné Dr. Kovács Piroska
jegyző

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A Tét Város Polgármesteri Hivatalának **Informatikai Biztonsági Szabályzatát** (továbbiakban IBSZ) a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló többször módosított 1992. évi LXIII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés alapján a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa a hivatalnál az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat olyan alacsonyabb szintű szabálygyűjtemény, amely azokat a gyakorlati kérdéseket helyezi előtérbe, amelyek konkrét cselekvési mintákat határoznak meg. Itt kell megfogalmazni azokat a célokat, amelyek elérése érdekében a szabályzat létre lett hozva, és ami miatt az intézménynél az informatikai biztonsággal foglalkozni kell. Az IBSZ a hivatal belső használatra szóló dokumentuma.

Az Informatikai Biztonsági Szabályzat célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működni kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen Informatikai Biztonsági Szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya a hivatal valamennyi fő- és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

2.2. Tárgyi hatálya

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

3. Az adatkezelés során használt fontosabb fogalmak

Személyes adat: a meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható;

Különleges adat:

- a) a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre,
- b) az egészségi állapotra, a kóros szenvedélyre, a büntetett előéletre vonatkozó személyes adat;

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységre vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől;

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy műveletek összessége, így pl. gyűjtése, felvétele, rögzítése, rendszerezése, tárolása,

megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel rögzítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérlenymat, DNS minta, íriszkép) rögzítése is.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából személyes adatok feldolgozását végzi.

Adatállomány: az egy nyilvántartó rendszerben kezelt adatok összessége.

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

A Hivatal alapbiztonsági fokozatba tartozik, általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési kézikönyv,
- Folyamatba épített előzetes és utólagos vezetői ellenőrzés rendszere.

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,

- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírászerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

6.2. A védelem eszközei

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

7. A védelem felelőse

A védelem felelőse a jegyző és a rendszergazda.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Hivatal adatvédelmi felelősének kell gondoskodnia.

7.1. A rendszergazda feladatai

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- ellátja az informatikai titokvédelmi munka szervezését és felügyeletét,
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,

- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- informatikai adatvédelmi feladatok ismertetése,
- a védelmi rendszer érvényesülésének ellenőrzése,
- felelős a hivatal informatikai rendszere hardver eszközeinek karbantartásáért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását.

7.2. A rendszergazda ellenőri feladatai

- évente egy alkalommal ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

7.3. A rendszergazda jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a hivatal vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthez valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

7.4. A rendszergazda személyének az alábbi követelményeknek kell megfelelnie:

- összeférhetetlenség – a rendszergazdai adatvédelmi felelős funkció összeférhetetlen minden olyan vezetői munkakörrel, amelyben adatvédelmi kérdésekben a napi munka szintjén dönteni, intézkedni kell.
- az informatikai hardver eszközök és a védelmi technikai berendezések ismerete,
- üzemeltetésben jártasság
- szervezőképesség
- az informatikai szakterületre vonatkozó jogi szabályozás ismerete.

7.5. A rendszergazda megbízatása

A rendszergazdát a jegyző bizza meg, aki jogosult ellátni a hatáskörébe tartozó feladatokat.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére a jegyző megbízottja biztosítja, erről nyilvántartást vezet.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint a hivatalnál a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

Az Informatikai Biztonsági Szabályzat folyamatos karbantartása a jegyző feladata.

8.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az információhoz való hozzáférést a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.

A naplófájlokat *havonta* át kell tekinteni, és a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a *rendszergazda* felelős.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. (1. sz. melléklet)

Az adatkezelési nyilatkozat naprakészen tartásáért a jegyző a felelős.

A titkot képező adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

9. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

9.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
 - földrengés,
 - árvíz,
 - tűz,
 - villámcsapás, stb.
- Környezeti kár:
 - légszennyezettség,
 - nagy teljesítményű elektromágneses térerő,
 - elektrosztatikus feltöltődés,
 - a levegő nedvességtartalmának felszökése vagy leesése,
 - piszkolódás (pl. por).
- Közüzemi szolgáltatásba bekövetkező zavarok:
 - feszültség-kimaradás,
 - feszültségingadozás,
 - elektromos zárlat,

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai 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,
- a jelszó megváltoztatásának az elmulasztása,
- illegális másolattal vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,

- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az informatikai eszközök környezete, azok védelme

10.1. A szerver (szoba) minimális igénye

- a szervert a legbiztonságosabb, legvédettebb területre kell telepíteni,
- a lehető legkevesebb nyílászáróval kell rendelkeznie,
- a szerverek miatt célszerű klímaberendezést működtetni,
- váratlan áramkimaradás esetén a szervereket intelligens UPS–sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet.

10.2. A munkaállomásokra vonatkozó előírás

Csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót bezárva kell tartani.

10.3. Egyéb vagyonvédelmi előírások

- szükséges kiépíteni egy zárható biztonságos helyiséget szerverszoba céljára,
- csak az illetékes dolgozók tartózkodhatnak a gépteremben,
- munkaidőn túl a szerverhelyiségben csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a szerverhelyiségbe történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

10.4. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (floppy, CD, DVD) 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 szervezetnek átadni csak engedéllyel szabad,

10.5. Vírus védelem

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.
- A hivatal dolgozói külső adathordozót csak abban az esetben csatlakoztathatnak a munkaállomásra, ha azt előzőleg egy a belső hálózattól független gépen, úgynevezett kapugépen vírusvédelmi szempontból ellenőrizték.
- A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát. Ha az adathordozón a vírusellenőrző program vírusot talált, nem engedhet másolást, futtatást, amíg a vírusoktól nem mentesítik az adathordozót.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.
- A felhasználók részéről tilos a vírusellenőrző szoftver beállításainak módosítása, különösképpen annak kikapcsolása.
- A vírusfertőzés lehetőségének csökkentése érdekében a tűzfalon és a levelező szerveren külön vírusvédelmi megoldás került telepítésre.

10.6. Tűzvédelem

A gépterem (szerverszoba) illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a gépteremre (*informatikai szobára*) vonatkozóan a hivatal Tűzvédelmi szabályzata tartalmazza.

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

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A gépteremben csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. leprellót).

A gépteremben dohányozni tilos!

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos pánccélszekrényben kell őrizni.

Ezen adatállományok kijelölése a *rendszergazda* feladata.

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

11.1. A gépterem (szerverszoba) védelme

Elemi csapás (*vagy más ok*) esetén a gépteremben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,

- biztonsági mentésekről, háttértákról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

11.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetés, karbantartás és szervizelés rendjét külön utasításban kell szabályozni.

A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.

A munkák szervezésénél figyelembe kell venni:

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

Alapgép szétbontását (kivéve a garanciális gépeket) csak a rendszergazda végezheti el. Billentyűzet, monitor, nyomtató cseréjének idejét dokumentálni kell.

11.3. Az informatikai feldolgozás folyamatának védelme

11.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftver védelme. A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
 - = a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
 - = az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- adatrögzítési folyamat bizonylatolása.

A másodlagos adathordozókat kísérő jeggyel kell ellátni melynek tartalma:

- témaazonosító, bizonylat neve,
- rekord (tételszám),
- rögzítést ill. ellenőrzést végző személyek nevei.

- adatrögzítés folyamatához kapcsolódó dokumentációk:
 - = adatrögzítési utasítások,
 - = ellenőrző rögzítési utasítások,
 - = tesztelő és törlő programok kezelési utasításai,
 - = megőrzési utasítások,
 - = gépkezelési leírások.

11.3.2. Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani.

Az informatikai eszközök üzemeltetéséért a rendszergazda felelős.

Köteles gondoskodni a feldolgozások igényeinek megfelelő mágneses adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni.

Az operációs rendszer adta lehetőségek figyelembe vételével biztosítani kell a külső és belső címek azonosságát.

A belső címke felépítésével illetve használatánál figyelembe kell venni a megőrzési időpont ellenőrzésének szükségességét (aktuális ellenőrzés).

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

11.3.3. Adathordozók tárolása

Az adathordozók tárolására a géptermén kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

Az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet.

11.3.4. Az adathordozók nyilvántartása

A mágneses adathordozókról 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.

A nyilvántartás vezetéséért a jegyző felelős.

11.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá hivatalunk Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza

meg.

11.3.6. Az adathordozók karbantartása

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

11.3.7. Selejtezés, sokszorosítás, másolás

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

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott) mágneslemezt, CD-t, DVD-t,
- véglegesen elhasználódott anyagot (*pl. leporelló*).

Az alkalmatlan mágneslemezeket, CD-ket, DVD-ket fizikai roncsolással használhatatlanná kell tenni.

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezésről (*3 példányban*) jegyzőkönyvet kell készíteni, melynek az alábbi adatokat kell tartalmaznia:

- a selejtezendő adathordozók tulajdonosának megnevezését,
- a selejtezés időpontját,
- milyen adathordozók, és azok mely adatai kerülnek selejtezésre,
- a selejtezést végzők aláírását.

A selejtezési jegyzőkönyvek nem selejtezhetőek.

Titkos adatokat tartalmazó adathordozókat selejtezni nem lehet, ezen adatokat tartalmazó adathordozókat a TÜK utasítása szerint kell kezelni.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. (*Az üzemi másolás nem minősül másolásnak.*)

Biztonsági illetve archív adatállomány előállítását másolásnak számít.

11.3.8. Leltározás

Az adathordozókat a Leltárkészítési és leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

A beszerzett, illetve üzemeltetett hardver és szoftver eszközök leltározása a Pénzügy feladata

11.3.9. Mentések, file-ok védelme

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.

A mentések folyamata:

- A mentéseket naponta, központi mentő szoftverrel kell végrehajtani.
- A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamint a tárolt adatoknak teljes körűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A szerverek esetében a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A szerverek mentését hetente, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.

A munkák során létrehozott szövegszerkesztő, táblázatkezelő és egyéb dokumentumok, valamint a levelek automatikusan mentésre kerülnek a központi fájlszerverről. A munkatársak munkájuk során kötelesek ennek a kialakított jogosultságrendszernek a használatára.

A személyi anyagok adatállományának mentését a humánpolitikai előadó havi gyakorisággal végzi el.

A főkönyvi könyvelés adatainak mentését a Pénzügy napi gyakorisággal végzi el.

A pénztár könyvelés adatainak mentését a Pénzügy napi gyakorisággal végzi el.

Az egyéb analitikus nyilvántartások adatainak mentését a Pénzügy heti gyakorisággal végzi el.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak.

11.4. Szoftver védelem

11.4.1. Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetőek legyenek a felhasználók számára.

Teendők a következők:

- az üzembiztonság érdekében tartalék operációs rendszerrel kell rendelkezni, amely szükség esetén azonnal betölthető legyen,
- a rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges,
- a rendszerszoftverben módosításokat kizárólag a rendszergazda végezhet,
- a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni,
- a változtatásokról nyilvántartást kell vezetni.

11.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

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

Minden felhasználónak jelszóval kell védenie a programját. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

A jelszavaknak az alábbi minimális követelménnyel kell rendelkeznie:

- A hálózati jelszó legalább 6 karakterből álljon, kis és nagybetűk, valamint számok, egyéb írásjelek közül legalább 2 típusút tartalmazzon.
- Az alkalmazáshoz szükséges jelszavaknak legalább 5 karakterből kell állni.
- A jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, vagy könnyen visszafejthető kifejezéssel.
- A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat havonta meg kell változtatniuk.
- Ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.
- A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt jelszóval.
- A jelszót nem szabad több személy között megosztani.
- A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.
- A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.

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

Lokális gépekre programot csak a rendszergazda tudtával lehet telepíteni.

A telepítést dokumentálni kell. A dokumentálásnak tartalmaznia kell azt, hogy milyen programot, mikor és ki telepített fel a számítógépre.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

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

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

A program dokumentáció a rendszerdokumentációnak része.

Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni,
- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

Programok fizikai védelme

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

12. A központi számítógép(ek) és a hálózat munkaállomásainak működésbiztonsága

12.1. Kiszolgálók

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A központi gépek háttértáiról naponta biztonsági mentést kell készíteni. A mentés mentőszoftver segítségével szalagos meghajtóra készül.

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.

12.2. Munkaállomások

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet. Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

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.

Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

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

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A munkaállomások tekintetében az alábbi rendelkezéseket is be kell tartani:

- A munkaállomások nincsenek jól védhető helyen, ezért védelműkről szoftver úton gondoskodni kell.
- Ha a felhasználó napközben magára hagyja a gépet, zárolást, vagy jelszavas képernyővédőt kell alkalmaznia.
- Ha a felhasználó munkaviszonya megszűnik, akkor felhasználói azonosítóját meg kell szüntetni.

13. Internet hozzáféréssel kapcsolatos intézkedések

A hivatal rendelkezhet internet elérési lehetőséggel.

Az internet eléréseket biztosító számítógépekre a helyi hálózatra nem kapcsolódó munkaállomásokra vonatkozó szabályok érvényesek.

Az internetes gépen minden esetben működtetni kell a vírusvédelmet.

A vírusok és az illetéktelen hozzáférések miatt célszerű tűzfalat konfigurálni.

A tűzfal működése közben keletkező állományokat az üzemeltetőnek rendszeresen ellenőrizni kell.

A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztését a jegyző szabályozza

14. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.

A folyamatba épített előzetes és utólagos vezetői ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

15. Záró rendelkezések

**Az Informatikai Biztonsági Szabályzat
2010. év december hó 22. napjával lép hatályba.**

A Képviselő-testület a szabályzatot a 188/2010. (XII. 22.) számú határozatával fogadta el. A szabályzatot Tét Város Önkormányzat Képviselő – testülete a 2010. december 22-ei ülésen fogadta el.

A szabályzathoz kapcsolódó adatkezelési nyilatkozatot a köztisztviselők aláírásukkal hitelesítik.

Tét, 2010. december 22.

P.H.

.....
Dr. Kukorelli László

.....
Bereczkiné Dr. Kovács Piroska

polgármester

jegyző

Tét Város Polgármesteri Hivatal

ADATKEZELÉSI NYILATKOZAT

Alulírott (név)
..... (lakcím)

nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáférése kísérletet sem teszek.

Dátum: 20.....

.....
aláírás