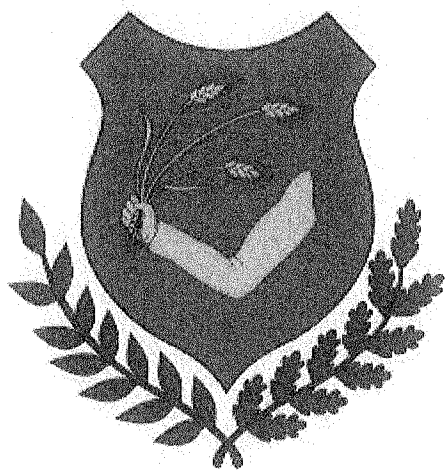
Nyt.: 2/2013/INF.

ABONY VÁROS ÖNKORMÁNYZAT



Informatikai Biztonsági Szabályzat

Hatályos: 2007. 12. 01.

2/2013/ INF.

Abonyi Polgármesteri Hivatalának szabályzata

az informatikai biztonságról

Az Abonyi Polgármesteri Hivatal (továbbiakban: Hivatal) 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, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint az államtitkok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés alapján a következők szerint határozom meg.

I.
Általános rendelkezések

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

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 elhasználásból 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 működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.
A jelen Informatikai Szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2.) Az Informatika Biztonsági Szabályzat hatálya

Személyi hatálya

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

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 értelmező rendelkezések tekintetében az Avtv. 2. §-ának 1-21. pontjai az irányadóak a következők szerint:

1. *személyes adat:* bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) 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. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;

2. *különleges adat:*

***a)* a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra,**

***b)* az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat;**

3. *bűnügyi személyes adat:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

4. *közérdekű adat:* az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső,

bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől;
5. *közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
6. *hozzájárulás:* az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;
7. *tiltakozás:* az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;
8. *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;
9. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például 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 készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is;
10. *adattovábbítás:* ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik;
11. *nyilvánosságra hozatal:* ha az adatot bárki számára hozzáférhetővé teszik;
12. *adattörlés:* az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;
13. *adatzárolás:* az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;
14. *adatmegsemmisítés:* az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;
15. *adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;
16. *adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából - beleértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi;
17. *személyesadat-nyilvántartó rendszer (nyilvántartó rendszer):* személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető;
18. *adatállomány:* az egy nyilvántartó rendszerben kezelt adatok összessége;
19. *harmadik személy:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

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

II.
Az informatikai Biztonsági Szabályzat biztonsági fokozata

1.) A hivatalunk fokozott biztonsági fokozatba tartozik, az elektronikus információs rendszer biztonsági osztálya: 2.

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

- Szervezeti és Működési Szabályzat
- Belső ellenőrzési kézikönyv
- Adatvédelmi szabályzat

III.
A 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 ható tényezők:

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

1.) 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 terlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

2.) A védelem eszközei:

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

IV.
A védelem felelőse

A védelem felelőse, az elektronikus információs rendszer biztonságáért felelős személy a LEADER Kft. rendszergazdája.

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

1.) Adatvédelmi felelős (rendszergazda) :

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- ellátja az informatikai titokvédelmi munka szervezését, 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 újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- a Szervezeti és működési Szabályzat adatvédelmi szempontból való véleményezése,
- az adatvédelmi feladatok ismertetése, oktatása,
- a védelmi rendszer érvényesülésének ellenőrzése,
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- felelős a hivatal informatikai rendszere hardver eszközeinek karbantartásáért, az időszakos hardver tesztjeiért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer önadminisztrációját,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- tevékenységéről folyamatosan beszámol a hivatal vezetőjének.
- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,

- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a hivatal vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet 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.

2.) Az adatvédelmi felelős megfelel az alábbi követelményeknek:
- erkölcsi feddhetetlenség,
- összeférhetetlenség – az 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,
- szervezőkészség,
- szakterületre vonatkozó jogi szabályozás ismerete.

3.) Az adatvédelmi felelőst a jegyző bízza meg.
Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

V.
Az Informatikai Biztonsági Szabályzat alkalmazása

Az informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére az adatvédelmi felelős oktatás formájában biztosítja. Erről nyilvántartást vezet.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az Informatikai Biztonsági Szabályzat előírásainak megfelelően.

A szabályzatot az informatikában – valamint a hivatalnál – a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az informatikai Biztonsági Szabályzat folyamatos karbantartása az adatvédelmi felelős feladata.

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.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.
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 lemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
A naplófájlokat havonta át kell tekinteni, s a jogosulatlan hozzáférést vagy annak kísérletét az hivatal vezetőjének azonnal jelenteni kell.
A naplófájlok áttekintéséért, értékeléséért a rendszergazda 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 berendezéseken kiépített technikai megoldásokkal is biztosítani kell. (szoftver, hardver adatvédelem).

VI.
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.

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

2.) Emberi tényezőkre visszavezethető veszélyek:
- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok)
- figyelmetlenség (ellenőrzés hiánya),

- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a jelszó gyakori (napi, heti) megváltoztatásának az elmulasztása,
- a megváltozott körülmények figyelmen kívül hagyása,
- 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.

VII.
Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

1.) A tervezés és előkészítés során előforduló veszélyforrások
- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, ellenőrzési szempontok hiányos betartása

2.) A rendszerek megvalósítása során előforduló veszélyforrások:
- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

3.) A működés és fejlesztés során előforduló veszélyforrások:
- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

VIII.
Az informatikai eszközök környezetének védelme

1.) Vagyonvédelmi előírások
- az informatikai szoba helyiségét biztonsági zárakkal kell felszerelni,
- az informatikai szobába való be-és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak az informatikai szobában
- munkaidőn túl az informatikai szobában csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- az informatikai szobába való illetéktelen behatolás tényét a hivatal vezetőjének azonnal jelenteni kell.

- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

2.) Az adathordozókat
- 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 (pendrive, CD) 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,
- a munkák befejeztével a használt berendezést és környékét rendbe kell tenni.

3.) Tűzvédelem

Az informatikai szoba illetve a kiszolgáló helyiség „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A tűzvédelem feladatait, sajátos előírásokat az 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.

A hivatal azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.

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

A informatikai szobában csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad használni (pl. leporelló)

A gépteremben dohányozni tilos!

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

Ezen adatállományok kijelölése a rendszergazda feladata.

IX.
Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

1.) Az informatikai szoba védelme

Elemi csapás esetében az informatikai szobában bekövetkezett részleges vagy teljes károsodáskor sürgősen el kell végezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatokat vissza kell állítani,
- új adatfeldolgozást, helyiségeket ki kell alakítani,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

2.) Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetés, karbantartás és szervízelés 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.

3.) Az informatikai feldolgozás folyamatának védelme

Az adatbevitel hibátlan műszaki állapotú berendezésen történhet.

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.

A bejelentési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. A tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá.

Az adatok bevitele során alapelv, hogy azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A szerver rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontását dokumentálni kell.

4.) 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 alkalmazásáért 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 formában 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 szükségszerűségét (aktuális ellenőrzés).

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

5.) Adathordozók tárolása
Az adathordozók tárolására az informatikai szobán kívüli műszaki-, tűz-, és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

Mágneses adathordozót a részlegből ki-, illetve oda bevinni csak az üzemeltetésért felelős vezető engedélye alapján lehet.

6.) Az adathordozók nyilvántartása
A mágneses adathordozókról nyilvántartást kell vezetni.

7.) Az adathordozók megőrzése
Az adathordozók megőrzési idejét a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI.

törvényben foglaltak, továbbá hivatalunk Iratkezelési Szabályzatában foglaltak alapján az adatkezelő határozza meg.

8.) Az adathordozók karbantartása

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

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

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

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

A selejtezést a hivatal Selejtezési Szabályzata, valamint Iratkezelési Szabályzata alapján kell folytatni.

Sokszorosítás, másolást csak az érvényben lévő rendeletek szerint szabad végezni.

Biztonsági illetve archív adatállomány előállítása másolásnak számít.

10.) Leltározás

Az adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

11.) Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.

A szerveren működő WEB oldalak mentése a LEADER Kft. rendszergazdájának feladata. A mentést minden módosítás után el kell végezni.

A mentést meghatározott időszakonként el kell végezni.

A munkák során létrehozott word és excel dokumentumok mentése a LEADER Kft. rendszergazdájának feladata.

A személyi anyagok adatállományának mentését havi gyakorisággal végzi el.

A főkönyvi könyvelés adatainak mentését heti gyakorisággal végzi el.

A pénztár könyvelés adatainak mentését heti gyakorisággal végzi el.

Egyéb analitikus nyilvántartások adatainak mentését heti gyakorisággal a rendszergazda végzi el.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adathordozókról másolatot kell időnként készíteni.

A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

12.) Rendszerszoftver védelem

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

Az üzembiztonság érdekében tartalék operációs rendszerrel kell rendelkezni, amely szükség esetén rögtön betölthető legyen.

A rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges.

Név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek.

A módosítással egy időben, a dokumentációban is a változásokat át kell vezetni.

A változásokról nyilvántartást kell vezetni.

13.) Programhoz való hozzáférés, programvédelem

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

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 a neve,
- a feldolgozási rendszer megnevezése.

A program dokumentáció a rendszerdokumentációnak része.

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

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

A programok nyilvántartásáért és működőképes állapotban tartásáért a rendszergazda felelős.

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

A felhasználói jogosultságok felhasználónkénti meghatározása (felhasználói programok, alkalmazások, hálózati megosztások és eszközök) a szervezeti vezető javaslatára a jegyző jóváhagyásával kerül sor a 2. sz. melléklet szerinti jogosultság-nyilvántartó lapon.
A jogosultságok beállítása a rendszergazda és az alkalmazás adminisztrátorának a feladata.
A felhasználókról és a kapott jogosultságokról a Hatósági Osztály kijelölt munkatársa nyilvántartást vezet.
A rendszerekben történő változások miatt a jogosultságok módosításának kezdeményezése a rendszergazda és az alkalmazás adminisztrátor feladata.
A felhasználók személyében történő változás esetén a jogosultságok meghatározását a szervezeti egység vezetője kezdeményezi.

A felhasználói jogosultságok felülvizsgálata folyamatos, a működő rendszerek és az ellátandó feladatok függvényében. Felelős a szervezeti egység vezető.

14.) Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletességű dokumentálásnak.
A dokumentációról nyilvántartást kell vezetni, s ennek az alábbiakat kell tartalmaznia:

- rendszer megnevezése
- dokumentáció típusa

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

X.
A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

1.) Központi gép (Szerver)

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

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 esetén adaptálni kell, és tesztadatokkal ellenőrizni kell a működésüket.
A Hivatal informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

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

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

XI.
Ellenőrzés

A Hivatal éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.
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 munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását a Titkárság vezetője folyamatosan ellenőrzi.

XII.
Záró rendelkezések

A szabályzat 2007. december 1. napján lép hatályba.

Abony, 2007. november „30".

Dr. Németh Mónika
jegyző sk.

Záradék

Aktualizálva a módosításokkal, egységes szerkezetbe foglalva.

Abony, 2013. december 10.

Jóváhagyta: Dr. Balogh Pál
Jegyző

Abony Város Jegyzője

GÉPTERMI REND

1. sz. melléklet

1. Az informatikai szobában az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:
   - a jegyző,
   - osztályvezetők,
   - szervezők, programozók, műszaki szakemberek.

Más személyek benntartózkodását csak a jegyző engedélyezheti.

2. Üzemeltetés alatt az ajtókat állandóan becsukva, üzemidőn kívül pedig zárva kell tartani és a kulcsokat le kell adni.
   A gépterem kulcsát csak a jegyző által összeállított külön listán szereplő személyek kaphatják meg.
   Munkaidőn kívül idegen személy csak a hivatal vezetőjének (távollétében helyettesének) engedélyével tartózkodhat az informatikai szobában.
   Az informatikai szoba áramtalanításáért a rendszergazda felelős.

3. Az informatikai szobában az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni. A géptermi rend megtartásáért és a biztonságos műszaki üzemeltetésért a rendszergazda felelős.
4. A gépterembe ételt, italt bevinni és ott fogyasztani TILOS!
5. SZIGORÚAN TILOS a gépteremben égő cigarettával belépni, illetve ott dohányozni.
6. Az informatikai szoba takarítását csak az arra előzőleg kioktatott személyek végezhetik.
7. A berendezések belsejébe nyúlni TILOS. Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazda végezheti.
8. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.
9. Az informatikai szobában elhelyezett adathordozókhoz a rendszergazdán kívül, illetve engedélye vagy jelenléte nélkül senki nem nyúlhat.
10. Adathordozókat csak a rendszergazda engedélyével lehet kihozni illetve bevinni az informatikai szobába.
11. Az elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet.
12. Az informatikai szobában elhelyezett jelzőberendezések műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak, és bármilyen rendellenességet észlelnek azonnal jelenteni kell a működésükért felelős megbízottnak.
13. A gépteremben egyszerre legalább egy, a gépek kezeléséhez értő személynek kell tartózkodnia. Üzemben lévő géptermet felügyelet nélkül hagyni nem szabad.
14. A javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, szakszerűség, a

vonatkozó érintésvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, amely nem elégíti ki a balesetvédelmi előírásokat.

A fenti rendelkezések megsértése esetén fegyelmi felelősségre vonás kezdeményezhető.

Név: Felhasználó

Gép azonosítója:

Osztály:

Saját e-mail cím:

Egyéb megjegyzés:

Közös e-mail címek:

- titkarsag ☐
- abony ☐
- regi-abony ☐
- anyakonyv ☐
- gazdasigiosztaly ☐
- adohatosag ☐
- telepulesfejlesztes ☐
- hatszoc ☐

Hálózati mappák:

- ELOTER ☐
- JEGY ☐
- GAZD ☐
- ADÓ ☐
- TER ☐
- SZOC ☐
- HAT ☐
- EPHAT ☐
- ADATOK ☐
- HIVATAL ☐
- JOGTAR ☐
- HOME ☐

Telepített programok

Firefox	☐	PDF-Xview	☐
ThunderBird	☐	PDF Creator	☐
Chrome	☐	AutoCAD LT	☐
Word	☐	Totalcomm	☐
Excell	☐	DWG Viewer	☐
Explorer	☐	Foxit	☐
InfranView	☐	I-View	☐
Adobe AR	☐	Adobe Reader	☐
DWGSee Pro	☐		
DWG True View	☐		
		Adobe Reader	☐

Gép adatai:

- Win 2000 ☐
- Win XP ☐
- Win 7 ☐
- Win 8 ☐
- Internet ☐
- Hálózati m áll ☐

	Jogosultság	Módosítás		Jogosultság	Módosítás
Bérfejlesztés			HHH Nyilvánt		
Önegem			Jelent		
Árinfó stat			CSTInfo		
Befesz			Statisztika		
Kati			Visual reg		
eKata			Optijus	Felhasználó	
ebr42			NJT		
KIR Stat			MikroVoks32		

Név Felhasználó

	Jogosultság	Módosítás		Jogosultság	Módosítás
KIR			NFÜ		
KSH Elektra			Elektra		
Terka			Önkado		
Sziszi			Foka		
Kasper	Felhasználó		EDTR		
ANYK			Takarnet		
Microsec e-signo			Civil Üzlet		
Etrius			Winszoc		
E adat			ASZA		
KGR 11			B2Net		
P üadatszolg			Közigállás		
			WinEb		

Jegyző aláírása | Dolgozó aláírása | Osztályvezető aláírása

Kelt:

Módosítás

Jegyző aláírása | Dolgozó aláírása | Módosítást végző személy aláírása

Kelt: