

***A FELCSÚTI KÖZÖS ÖNKORMÁNYZATI  
HIVATAL***

***INFORMATIKAI BIZTONSÁGI SZABÁLYZATA***

***Hatályos: 2013. március ... napjától***

## **INFORMATIKAI BIZTONSÁGI SZABÁLYZAT**

*A Felcsúti Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 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, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.*

*Az Informatikai Biztonsági Szabályzat célja továbbá:*

- a titok-, munka, 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**

**érintett:** *bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;*

**személyes adat:** *az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;*

**különleges adat:** *a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;*

**közérdekű adat:** *az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;*

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

**adatkezelő:** *az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt 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 a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

**adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

**nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;

**adattörlés:** az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

**adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

**adatzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

**adatmegsemmisítés:** az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

**adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

**adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi;

**adatfelelős:** az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

**adatközlő:** az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közlésezi;

**adatállomány:** az egy nyilvántartásban kezelt adatok összessége;

#### **4. Az IBSZ biztonsági fokozata**

Hivatalunk alapbiztonsági fokozatba tartozik.

Hivatalunk 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,*
- *Belső kontroll rendszer.*

## **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, 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 rendszergazda.*

*A jelen szabályzatban foglaltak szakszerű végrehajtásáról a rendszergazdának kell gondoskodnia.*

### **7.1. A rendszergazda- adatvédelmi felelős feladatai**

- *ellátja az adatfeldolgozás felügyeletét,*
- *ellenőrzi a védelmi előírások betartását,*
- *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,*
- *felelős a Hivatal informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,*
- *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 biztonság szempontjából a lényeges paraméterek alakulását,*
- *ellenőrzi a rendszer önadminisztrációját,*
- *javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,*
- *tevékenységéről rendszeresen beszámol a jegyzőnek.*

### **7.2. A rendszergazda- adatvédelmi felelős ellenőri feladatai**

- *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.*

### **7.3. A rendszergazda- adatvédelmi felelős jogai**

- *az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény 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.*

#### **7.4. Rendszergazda- adatvédelmi felelős kiválasztása**

*Az alábbi követelményeknek kell megfelelnie:*

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

#### **7.5. A rendszergazda- adatvédelmi felelős megbízatása**

*Az adatvédelmi felelőst a jegyző bízta meg.*

*Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.*

### **8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja**

*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 IBSZ előírásainak megfelelően.*

#### **8.1. Az Informatikai Biztonsági Szabályzat karbantartása**

*Az IBSZ-t a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.*

*Az Informatikai Biztonsági Szabályzat folyamatos karbantartása a rendszergazda- adatvédelmi felelős feladata.*

*E tevékenységről, annak konkrét tartalmáról évente egyszer írásbeli beszámolót kell készíteni.*

## **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 a jegyző.*

*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.*

*Minősített adatok esetén, 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, s a jogosulatlan hozzáférést vagy annak a kísérletét a jegyzőnek 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 rendszergazda 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 eszközbizist 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,
- csőtörés.

## **9.2. Emberi tényezőre visszavezethető veszélyek**

**Szándékos károkozás:**

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtevesztő 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 gyakori 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.*

## **10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek**

### **10.1. 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.*

### **10.2. A rendszerek megvalósítása során előforduló veszélyforrások**

- *hibás adatállomány működése,*
- *helytelen adatkezelés,*
- *programtesztelés elhagyása.*

### **10.3. A működés és fejlesztés során előforduló veszélyforrások**

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

## **11. Az informatikai eszközök környezete, azok védelme**

### **11.1. A szerverszoba minimális igénye**

- a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,*
- a lehető legkevesebb nyílászáróval kell rendelkeznie,*
- váratlan áramkimaradás esetén a szervereket intelligens UPS–sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet.*

### **11.2. A munkaállomásokra vonatkozó előírás**

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

### **11.3. Egyéb vagyonvédelmi előírások**

- *a gépterem (szerverszoba) külső és belső helyiségeit biztonsági zárral kell felszerelni,*
- *a szerverszobába való be- és kilépés rendjét szabályozni kell,*
- *csak az illetékes dolgozók tartózkodhatnak a gépteremben,*

- a szerverszoba kulcsának felvétele, illetve leadása csak aláírás ellenében történhet,
- munkaidőn túl a szerverszobában csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a szerverszobába 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.

#### **11.4. 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, pendrive) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feladatokhoz szükségesek,
- adathordozót más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

#### **11.5. Vírusvédelem**

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.
- 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.

#### **11.6. 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.*

*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 munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.*

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

*A gépteremben dohányozni tilos!*

*A gépteremben, valamint a munkaállomásoknál ételt, italt fogyasztani 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.*

## **12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek**

### **12.1. 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.*

### **12.2. 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.*

## **12.3. Az informatikai feldolgozás folyamatának védelme**

### **12.3.1. 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 bevitelénél során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

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

- 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.

### **12.3.2. 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 a 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.*

### **12.3.3. Adathordozók tárolása**

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

*Mágneses adathordozót a részlegből ki-, illetve oda bevinni csak a **Körjegyző** engedélye alapján lehet.*

### **12.3.4. Az adathordozók nyilvántartása**

*Az adathordozókról nyilvántartást kell vezetni.*

*A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.*

*A nyilvántartás vezetéséért: a titkársági referens a felelős.*

### **12.3.5. 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 a Hivatal Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.*

### **12.3.6. Az adathordozók karbantartása**

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

### **12.3.7. 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) mágneslemez, CD-t, DVD-t, pendrive-t.*
- véglegesen elhasználódott anyagot (pl. leporelló).*

*Az alkalmatlan mágneslemezeket, CD-eket, DVD-eket, pendrive-eket 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.*

#### **12.3.8. Leltározás**

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

#### **12.3.9. 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 az adatokat legalább 2 példányban kell menteni, és egymástól fizikailag elkülönült helyiségben elzárt, a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.*
- A szerverek mentését legalább hetente, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni.*
- A szerveren működő WEB oldalak mentése a rendszergazda feladata. A mentést minden módosítás után el kell végezni.*
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.*

*Az egyéb mentéseket meghatározott időszakonként el kell végezni.*

*A munkák során létrehozott dokumentumok mentése az azt létrehozó munkatársak feladata.*

*A főkönyvi könyvelés adatainak mentését napi gyakorisággal a költségvetési ügyintéző végzi el.*

*A pénztár könyvelés adatainak mentését napi gyakorisággal a pénztáros végzi el.*

*Az egyéb analitikus nyilvántartások adatainak mentését napi gyakorisággal költségvetési ügyintéző végzi el.*

*A levelezések mentését a felhasználó 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 a jegyző engedélyével adhatók ki.*

## **12.4. Szoftver védelem**

### **12.4.1. Rendszerszoftver védelem**

*A **Körjegyzőnek** 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,*
- 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 változtatásokról nyilvántartást kell vezetni.*

### **12.4.2. 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 8 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 5 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.
- A jelszavakat, valamint a munkaállomások BIOS jelszavát lezárt, aláírt és lepecsételt borítékban páncélszekrényben (lemezszekrényben) kell tárolni, lehetőleg a vezető irodájában.

*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 rendszer-dokumentációnak része.*

### **Programok megőrzése, nyilvántartása**

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

*A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a Hivatal az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.*

*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 való tartásáért a rendszergazda a felelős.*

### **Programok fizikai védelme**

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

## **12.5. Dokumentálás**

*Kiemelkedő szerepe van a megfelelő szintű és részletezettségű dokumentálásnak.*

*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.*

## **13. A központi számítógépek és a hálózat munkaállomásainak működésbiztonsága**

### **13.1. Központi gépek (Szerver)**

*Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültség-ingadozásoktól, áramkimaradás esetén adatvesztéstől.*

*A központi gépek háttértáiról hetente egy teljes, a többi napon különbségi biztonsági mentést kell készíteni. A mentéseket heti egy alkalommal külső adattároló egységre kell másolni. Az így keletkezett heti mentéseket 5 évig meg kell őrizni.*

*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.*

### **13.2. Munkaállomások (USER-ek)**

*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 védelmükről 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.*

#### **14. Internet hozzáféréssel kapcsolatos intézkedések**

*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 tűzfalat kell konfigurálni.*

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

*A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztését a jegyző határozza meg.*

#### **15. 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 folyamatba épített előzetes, utólagos és vezetői ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.*

## **16. Záró rendelkezések**

*Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.*

*A szabályzatot jogszabályi vagy szervezeti változás esetén módosítani kell.*

*A munkaköri leírások elkészítésért, aktualizálásáért az igazgatási ügyintéző a felelős.*

***Az Informatikai Biztonsági Szabályzat  
2013. év március hó 1. napjával lép hatályba.***

*Felcsút, 2013. március 1.*

***Dr. Sisa András  
jegyző***

.....  
*Hivatal megnevezése*

**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: 201.* .....

.....  
*aláírás*

## **GÉPTERMI REND**

1. A gépteremben (szerverszobában) és az adatrögzítő helyiségében az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:

- a Körjegyző,
- Aljegyző,
- 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 az intézmény vezetőjének (távollétében helyettesének) engedélyével tartózkodhat a gépteremben.

A gépterem és az adatrögzítő helyiség áramtalanításáért a titkársági referens a felelős.

3. A gépteremben az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni. A géptermi rend megtartásáért a rendszergazda, a biztonságos műszaki üzemeltetésért szintén a rendszergazda a felelős.

4. A gépterembe ételt, italt bevinni és ott elfogyasztani TILOS !

5. SZIGORÚAN TILOS a gépteremben égő cigarettával belépni, illetve ott dohányozni!

6. A gépterem takarítását csak az arra előzőleg kioktatott személyek végezhetik.

7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazda végezheti. Ez alól csak a szervizek szakemberei kivétel.

8. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.

9. A gépteremben elhelyezett adathordozókhoz a rendszergazda, a Körjegyző és az Aljegyző, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.

10. Mágnesszalagokat, mágneslemezeket, mágnes kazettákat, CD és DVD lemezeket, pendrive-eket, leporellókat csak a rendszergazda, a Körjegyző és az Aljegyző engedélyével lehet kihozni, illetve bevinni a gépterembe.

11. *Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet!*
12. *A gépteremben elhelyezett jelzőberendezések (klíma, tűz- és betörésjelző) műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak, és bármilyen rendellenességet észlelnek azonnal jelenteni kell a működésükért felelős megbízottaknak.*
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, a szakszerűség, a vonatkozó érintésvédelmi 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.*