Adatvédelmi szabályzat

Készítette: Hernádi Csilla gazdasági vezető	
Iktatószám:	**Dátum: 2017. április 10.**
Érvényesség: határozatlan időre	**Jóváhagyta: Riszter Jánosné** **igazgató**
Készült: 5 db nyomtatott példányban	**Oldalak száma:**
Kapják: – igazgató – gazdasági vezető – könyvelők – pénztáros – ügyintézők	**Megjegyzés:** ez a példány sokszorosítható
Tárolási hely: az Intézmények Gazdasági Hivatalának hivatalos helyisége	

I.

AZ ADATVÉDELMI SZABÁLYZAT CÉLJA,

A szabályzat az intézmény működése során keletkező legfontosabb adatvédelmi, informatikai biztonsági szabályokat tartalmazza (különleges tekintettel az adatkezeléssel, adattovábbítással és nyilvánosságra hozatallal kapcsolatos adatvédelmi követelményekre.

A szabályzat hatálya kiterjed az Intézmények Gazdasági Hivatala közalkalmazottaira.

Az IGH könyvelési körébe tartozó intézmények az adatvédelmi szabályzatot maguk alakítják ki.

I. A személyi iratok kezelés és ezek adatvédelmi szabályai

Általános szabályok:

1. Személyi iratként kell kezelni bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett minden olyan adathordozót, amely a közalkalmazotti jogviszony:
- létesítésekor,
-fennállása alatt,
-megszűnésekor,
-illetve azt követően keletkezik és a közalkalmazott személyével összefüggésben adatot, megállapítást tartalmaz.

2. Az 1. pont alapján személyi irat:
a/ a személyi anyag iratai (a továbbiakban személyzeti irat),
b/ a közalkalmazotti jogviszonnyal összefüggő iratok,
c/ a közalkalmazottnak a közalkalmazotti jogviszonyával összefüggő más jogviszonyaival kapcsolatos iratok,
d/ a közalkalmazott saját kérelmére kiállított vagy önként átadott adatokat tartalmazó iratok.

3. A közalkalmazott közalkalmazotti jogviszonyával kapcsolatos iratok közül az alábbi iratok tartoznak személyzeti iratok közé:
- adatnyilvántartó lap,
-önéletrajz
-erkölcsi bizonyítvány,
-kinevezés,
-besorolásról rendelkező irat,
-áthelyezésről rendelkező irat,
-minősítés,
-a közalkalmazotti jogviszonyt megszüntető irat,
- a hatályban lévő büntetést kiszabó határozat,
-a közalkalmazotti igazolás másolata.

4. A személyi iratokat adott személyre vonatkozóan együttesen kell tárolni.

5. A személyi iratokat az intézmény iktatókönyvében iktatni kell. A beiktatott személyzeti iratokat tartalmuknak megfelelően csoportosítva, keletkezésük sorrendjében, az e célra személyenként kialakított gyűjtőben kell őrizni.

6. A személyzeti iratra csak olyan adat és megállapítás vezethető, amelynek alapja:
- közokirat vagy a közalkalmazott írásbeli nyilatkozata,
-a munkáltatói jogkör gyakorlójának írásbeli rendelkezése,
-bíróság vagy más hatóság döntése,
-jogszabályi rendelkezés.

7. A közalkalmazotti jogviszony megszűnése után a közalkalmazott személyi iratait a páncélszekrényben kell elhelyezni. Az így irattározott anyagokat a „ megszűnt" csoportban kell tárolni, hogy az elkülönítés biztosítva legyen.
8. A személyi iratok tárolási módja megegyezik a közalkalmazotti nyilvántartás tárolási módjával.
9. A közérdekű adatokon túl a közalkalmazott nyilvántartott adatairól tájékoztatás nem adható, személyi anyagát csak a Kjt. 83/D §-ában foglalt kivételes esetben lehet kiadni.
10. A személyi anyagokba való betekintésre jogosultak köre megegyezik a közalkalmazotti nyilvántartásba betekintésre jogosultak körével.

A személyi anyagok közül a pályázatokra vonatkozó speciális szabályok:

A pályázatok kezelési módja (Ha jogszabály, vagy munkaviszonyra vonatkozó szabály, illetve a munkáltató döntése alapján meghatározott munkakör betöltése pályázat alapján történik):

- A pályázatokat iktatni kell.
- A benyújtott pályázatokról a munkáltatói jogkör gyakorlója dönt. Kinevezni csak az a közalkalmazottat lehet, aki a pályázati eljárásban részt vett és a pályázati feltételeknek megfelelt.
- A benyújtott pályázat tartalma a pályázat elbírálásában résztvevőkön, valamint a közalkalmazotti alapnyilvántartásba betekinteni jogosultakon kívül csak a pályázó beleegyezésével közölhető harmadik személlyel.
- A pályázat eredményéről a pályázókat haladéktalanul, de legkésőbb 8 napon belül írásban kell tájékoztatni.
- Az eredménytelenül pályázóknak az értesítéssel együtt meg kell küldeni a teljes pályázati anyagukat is.
- Az iktatókönyvbe be kell vezetni a visszaküldés tényét.

II. A személyi iratokban szereplő személyes adatokat kezelők személyi felelősségéről

A személyi iratokban szereplő személyes adatokat kezelők személyes felelőssége az alábbiak szerint kerül meghatározásra:
a/ a személyi anyagban szereplő személyes adatok védelméért, az adatkezelés jogszerűségéért az intézményvezető a felelős,

b/ A személyi iratok vezetésével kapcsolatos feladatokat az intézményvezető által megbízott közalkalmazott látja el.

c/ A közalkalmazotti jogviszonnyal összefüggő adatok kezeléséért:

- az intézményvezető, mint munkáltató,
- a munkaügyi feladatok ellátásával megbízott dolgozó a személyi iratok kitöltéséért, iktatásáért, irattározásárt felelős
- a közalkalmazott saját adatainak közlése tekintetében tartozik felelősséggel.

d/ a személyi iratokban szereplő, nem közérdekű személyes adatokat csak a törvényben meghatározott esetekben és célokra, illetve az érintett közalkalmazott erre irányuló írásbeli kérelmére lehet felhasználni, illetve lehet átadni harmadik személynek.

A közalkalmazotti jogviszonnyal összefüggő adatok kezeléséért való felelősség tartalma:

1/ Az intézményvezető felel:
A közalkalmazotti jogviszonnyal összefüggő adatok védelmére és kezelésére vonatkozó jogszabályok, valamint az e szabályzatban rögzített előírások megtartásáért, illetve e követelmények teljesítésének ellenőrzéséért.

Felelősségi körében köteles gondoskodni:

- az adatvédelmi szabályzat folyamatos karbantartásáról,
- az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről,
- a közalkalmazotti jogviszonnyal összefüggő adatok védelmével kapcsolatos követelmények szerven belüli közzétételéről. A közzététel érdekében a közalkalmazottak kötelesek az adatvédelmi szabályzat megismerésére, majd ezt követően az erre vonatkozó nyilatkozat megtételére (ez utóbbit a szabályzat mellékleteként kell kezelni).

Felelősségei körében köteles intézkedni arról, hogy

- a személyi iratra történő adat rávezetés a megfelelő személyi iratra – az adat keletkezésétől, illetőleg változásától számított legkésőbb 8 munkanapon belül – rávezetésre kerüljön.
- A közalkalmazott által szolgáltatott és leigazolt adatok helyesbítését és kijavítását a közalkalmazott kérelmére történt kezdeményezés és igazolás alapján legkésőbb 8 munkanapon belül átvezessék,
- ha a közalkalmazott nem az általa szolgáltatott adatának kijavítását vagy helyesbítését kéri, akkor kezdeményeznie kell a munkáltatói jogkör gyakorlójánál az adathelyesbítést, illetve kijavítás engedélyezését. A munkáltatói jogkör gyakorlójának döntése alapján haladéktalanul el kell végezni a javítást.

2. A személyzeti feladatot ellátó közalkalmazott felelőssége:

- a személyi feladatot ellátó közalkalmazott alatt kell érteni minden olyan közalkalmazottat, aki az intézménynél tevékenysége során a közalkalmazotti nyilvántartással és személyi irattal összefüggő adatot kezel.
- A személyzeti feladatot ellátó közalkalmazott felelőssége gondoskodni arról, hogy az általa kezelt – közalkalmazotti jogviszonnyal összefüggő – adat és megállapítás az adatkezelés teljes folyamatában megfeleljen az e szabályzat I/6. Pontjában meghatározott iratok, valamint a jogszabályi rendelkezés tartalmának,
- a személyi iratra csak olyan adat, illetve megállapítás kerülhessen, amely e szabályzat I/6. Pontjában foglalt adatforrásokon alapul.

3/A közalkalmazott felelőssége:

- A közalkalmazott felelős azért, hogy az általa az intézmény részére átadott, bejelentett adatok hitelesek, pontosak, teljesek és aktuálisak legyenek.

III. Az adatvédelmi szabályok a nyilvántartások vezetési módszerei szerint

A hagyományos módszerrel végzett nyilvántartásokkal kapcsolatos adatvédelmi szabályok

A hagyományos módszerrel végzett nyilvántartásokkal kapcsolatban az alábbi alapvető adatvédelmi szabályokat kell betartani:

a/ gondoskodni kell a papír alapú adathordozók biztonságos tárolásáról. A tárolást zárható szekrényben kell megoldani.

b/ az adatokhoz való hozzáférést a tároló eszköz zárásával kell megoldani. A tárolók kulcsával csak azok a közalkalmazottak rendelkezhetnek, akik valamilyen személyzeti feladat ellátására feljogosítottak. A kiadott kulcsokról nyilvántartást kell vezetni. Amennyiben a kulcs elveszik, azt haladéktalanul jelenteni kell az intézményvezetőnek, aki gondoskodik a zár lecseréltetéséről.

c/ a nem rutinszerű, nem szokványos adatkezelésről, az adatkezelést megelőzően értesíteni kell az intézményvezetőt.

A számítógépes módszerrel végzett nyilvántartásokkal kapcsolatos adatvédelmi szabályok:

1. A szabályozás célja: biztosítani a számítógépes információs rendszerben az adatkezelés fizikai biztonságát, a működtetés rendjét.
2. Az adatbiztonság szabályozása keretében gondoskodni kell:

- a fizikai biztonság,
- az üzemeltetési biztonság, valamint az
- információtovábbítás biztonságáról.

2/1. A fizikai biztonság érdekében ellátandó feladatok:

- az adathordozó eszközök elhelyezésére csak olyan helyiség jelölhető ki, amely elegendő biztonságot nyújt az illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen.
- A számítástechnikai eszközök biztonsági megoldási dokumentációját az intézményvezető őrzi a páncélszekrényben.

2/2 Az üzemeltetési biztonság szabályairól:

- a számítástechnikai eszközök használatára felhatalmazott személyek névsorát - a feladatok meghatározásával- el kell végezni. A listát az intézményvezető állítja össze és őrzi.
- Külső személy (pl. karbantartás) számára a számítástechnikai eszközökhöz való hozzáférést lehetőleg úgy kell biztosítani, hogy a kezelt adatokat ne ismerhesse meg.
- A rendszerebe kerülő adatokat tartalmazó dokumentumokat biztonságosan kell kezelni, hogy azok el ne vesszenek, ne cserélődhessenek el, ne sérüljenek meg.

2/3 A technikai biztonság szabályai:

- az adatok és programok véletlen vagy szándékos megrongálását számítógépes biztonsági hozzáférési rendszerek alkalmazásával kell megakadályozni.
- Az adatállományok kezelése úgy kerül megszervezésre, hogy részleges vagy teljes megsemmisülés esetén tartalmuk rekonstruálható legyen, az adatállományok tartalmát képező adattételek számát az adatrögzítőnek

folyamatosan ellenőrizni kell. Az adatállományok kezelése során a munkaközi mentés eszközével is élni kell.

Az adatállományokról legalább két adathordozót kell készíteni, hogy az egyik megsemmisülése, sérülése esetén az eredeti adatok továbbra is rendelkezésre álljanak.

- A számítógépes üzemeltetés biztonsága számítógépes jelszóval védett programokkal történik.
- Az adatállományokban történt változásokat naplózni kell.
- Az adatbevitel során a bevitt adatok helyességét ellenőrizni kell.
- On-line adatmozgás kezdeményezésének jogosultságát ellenőrizni kell.
- Programfejlesztés vagy próba céljára valódi adatok felhasználását – ha a próbát külső szerv vagy személy végzi – el kell kerülni.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

1. Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ 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 működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembehelyezésen keresztül az üzemeltetésig.

A jelen IBSZ 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 kiterjed az IGH közalkalmazottaira.

2.2. Tárgyi hatálya

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

3. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

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

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

Adatkezelő: az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, i lletőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

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

Az IGH adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a vállalkozás belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:
Leltározási és értékelési szabályzattal,
Számviteli politikával

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:

- 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, előírásszerű felhasználására, reprodukálhatóságára,

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 az intézmény vezetőinek kell gondoskodnia.

7 .1. *Adatvédelmi felelősök feladatai*

a) Az igazgató feladatai a rendszergazdával egyeztetve:
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységét adminisztrálja.
- ellenőrzi a szoftverek használatának jogszerűségét

b) Rendszergazda feladatai:
- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a vállalkozás informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,

7.2. *Az intézményvezető feladatai, jogai*
- 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.

- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezetők a rendszergazda oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

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

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.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi 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 lehetőség szerint 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 rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a vállalkozás vezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.

Az 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,
- csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

1.1. behatolás az informatikai rendszerek környezetébe,
1.2. illetéktelen hozzáférés (adat, eszköz),
1.3. adatok- eszközök eltulajdonítása,
1.4. rongálás (gép, adathordozó),
1.5. megtévesztő adatok bevitele és képzése,
1.6. zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

1.7. figyelmetlenség (ellenőrzés hiánya),
1.8. szakmai hozzá nem értés,
1.9. a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
1.10. a megváltozott körülmények figyelmen kívül hagyása,
1.11. vírusfertőzött adathordozó behozatala,
1.12. biztonsági követelmények és gyári előírások be nem tartása,
1.13. adathordozók megrongálása (rossz tárolás, kezelés),
1.14. 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, adatelőkészítés, 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 környezetének védelme

11.1. Vagyonvédelmi előírások

– az irodák külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
– a szerverhez történő illetéktelen behatolás tényét az igazgatónak azonnal jelenteni kell,
– az informatikai eszközöket csak az igazgató által arra felhatalmazott alkalmazottk használhatják,
– az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

11.2. 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) 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 másnak átadni csak engedéllyel szabad,
– a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.3. Tűzvédelem

Az irodában elhelyezett számítógépekek miatt a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A számítógépek és szerverek védelme

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

– menteni a még használható anyagot,
– biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
– 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 üzemeltetést, karbantartást és szervizelést az informatikusok végzik.
A munkák szervezésénél figyelembe kell venni:
– a gyártó előírásait, ajánlatait,
– a tapasztalatokat.
Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

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 adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják 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 személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerver rendszergazda jelszavát az igazgató kezeli.

Az adatrögzítés folyamatához kapcsolódó dokumentációk:

- adatrögzítési utasítások,
- ellenőrző rögzítési utasítások,
- tesztelő és törlő programok kezelési utasításai,
- megőrzési utasítások,
- gépkezelési leírások.

12.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

12.3.3. Adathordozók tárolása

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

12.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

12.3.6. Selejtezés, sokszorosítás, másolás

A selejtezést a vállalkozás selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni.
Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

12.3.8. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

12.3.9. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazda a felelősek.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

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.

Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a vállalkozásoknak 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 vezetők a felelősek.

13. Záró rendelkezések

Jelen szabályzat 2017.04.10-tő lép hatályba.

Tata, 2017. április 10.

Riszter Jánosné
igazgató