PROSPERIS ALBA
KUTATÓKÖZPONT

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A dokumentum módosításainak jegyzéke
A dokumentum felülvizsgálatát kétévente szükséges elvégezni.

V1.1	**2026.05.01.**	**Módosított és egységes szerkezetbe foglalt dokumentum**	/2026. sz. ügyvezetői utasítás
V1.0	**2026.03.20.**	**Első verzió**	3/2026. sz. ügyvezetői utasítás
Verzió	**Dátum**	**Leírás**	**Hatályba helyező utasítás száma**

Tartalomjegyzék

1. Az Informatikai Biztonsági Szabályzat célja

A Prosperis Alba Kutatóközpont Nonprofit Kft. (a továbbiakban: Társaság) Informatikai Biztonsági Szabályzatának alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzat célja továbbá:

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

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának teljes időtartama alatt a megtervezésüktől kezdve az üzembehelyezésen keresztül az üzemeltetésig.

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 hatály

Az Informatikai Biztonsági Szabályzat személyi hatálya kiterjed a Társaság minden munkavállalójára, a Társasággal munkavégzésre irányuló egyéb jogviszonyban álló személyre, valamint az informatikai rendszert használó külső partnerekre.

2.2. Tárgyi hatály

Az Informatikai Biztonsági Szabályzat tárgyi hatálya kiterjed

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

3. Az adatkezelés során használt fontosabb fogalmak

***Adathordozó**: olyan eszközök összessége, amelyek alkalmasak az adatok tárolására, megőrzésére.*

***Informatikai eszközök**: olyan hardvereket, szoftvereket, hálózatokat és szolgáltatásokat jelent (eszközök), amelyek információk rögzítésével, kezelésével, rendszerezésével, továbbításával foglalkoznak.*

***Adatkezelés**: az adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.*

***Adatkezelő**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza (ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja).*

***Adatfeldolgozás**: az adatkezelő nevében végzett adatkezelés, köztük például adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik.*

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

***Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.*

***Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel*

***Adatvédelmi incidens:** a biztonság olyan sérülése, amely a továbbított vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.*

***Nyilvánosságra hozatal:** ha az adatot bárki számára hozzáférhetővé teszik.*

***Mobil eszköz:** hordozható kiépítésű, mikroprocesszor vezérlésű, operációs rendszerrel és háttértárolóval rendelkező informatikai eszköz (pl. laptop, notebook, PDA, táblagép, okostelefon).*

***Munkaállomás**: adatbevitelre és adatfeldolgozásra használt eszköz.*

4. Az Informatikai Biztonsági Szabályzat biztonsági fokozata

A Társaság adatai különböző biztonsági fokozatba tartozhatnak, úgymint üzleti titkok, pénzügyi adatok, továbbá 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

A jelen szabályzat előírásai összhangban vannak a Társaság alábbi szabályzataiban foglalt rendelkezésekkel:

a) Számviteli politika
b) Leltározási szabályzat
c) Szoftverek és könyvek vagyongazdálkodási szabályzata

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) az alkalmazott hardver eszközökre és azok működési biztonságára,
b) az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
c) az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
d) 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 a különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

7. A védelem felelőse

A védelem felelőse a Társaság ügyvezetője és a rendszergazdai feladatokat – szolgáltatási szerződés keretében – ellátó Önkormányzati Informatikai Központ Non-profit Kft. (a továbbiakban: ÖIK).
A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Társaság ügyvezetőjének kell gondoskodnia.

7.1. Adatvédelmi felelősök feladatai

a) Ügyvezető feladatai:
- a védett adatok körének meghatározása,
- az adatvédelmi feladatok ismertetése,
- az adatkezelés és adatfeldolgozás felügyelete,
- a védelmi előírások betartásának ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- a beszerzett, illetve üzemeltetett hardver és szoftver eszközök nyilvántartása.

b) A rendszergazdai feladatokat ellátó ÖIK feladatai:
- az Informatikai Biztonsági Szabályzat kezelése, naprakészen tartása, módosítások átvezetése,
- a saját feladatkörébe tartozó rendszer felügyelete,
- javaslattétel a rendszer szűk keresztmetszeteinek felszámolására,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
- a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a Tásaság informatikai rendszerének, hardver eszközeinek karbantartásáért,
- gondoskodik a folyamatos vírusvédelemről,
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a szoftverek használatának jogszerűségét,
- ellenőrzi a rendszer adminisztrációját.

c) Az adatvédelmi tisztviselő feladatai
- Ügyvezető segítése feladatai ellátásában
- ÖIK segítése feladatai ellátásában
- incidenskezelési eljárás működtetése, ideértve az információbiztonsági események, adatvédelmi incidensek (pl. adatvesztés, jogosulatlan hozzáférés) felismerését, dokumentálását és nyilvántartását,
- információbiztonsági és adatvédelmi tudatosság növelése, rendszeres oktatások és tájékoztatások szervezésével,
- külső szolgáltatók és adatfeldolgozók információbiztonsági és adatvédelmi megfelelőségének ellenőrzése, szerződéskötéskor.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

A jelen szabályzat előírásainak megismerését a Társaság munkavállalói részére az ügyvezető az ÖIK bevonásával, tájékoztatás formájában biztosítja.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az Informatikai Biztonsági Szabályzatot az informatikában, - valamint a Társaságnál - a fejlődés során bekövetkező változások miatt kétévente, illetve jelentős jogszabály vagy technológiai változásokkor aktualizálni kell.
A szabályzat folyamatos karbantartása a Társaság ügyvezetőjének a feladata.

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

Az adatok és információk jelentőségük és bizalmassági fokozatuk szerint kerülnek osztályozásra:

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

Az adatok feldolgozásakor meg kell határozni 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 külső eszközre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
A naplófájlokat rendszeresen át kell tekinteni, és a jogosulatlan hozzáférést vagy annak a kísérletét az ügyvezetőnek jelenteni kell.
A naplófájlok áttekintéséért az ÖIK, az értékeléséért a Társaság ügyvezetője a felelős.

Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, valamint 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

a) elemi csapás:
   - földrengés,
   - árvíz,
   - tűz,
   - villámcsapás stb.

b) környezeti kár:
   - légszennyezettség,
   - nagy teljesítményű elektromágneses térerő,
   - elektrosztatikus feltöltődés,
   - a levegő nedvességtartalmának felszökése vagy leesése,
   - piszkolódás (pl. por).

c) közüzemi szolgáltatásban bekövetkező zavarok:
   - feszültség-kimaradás,
   - feszültségingadozás,
   - elektromos zárlat,
   - csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

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

b) Nem szándékos, illetve gondatlan károkozás:
- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- 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, 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 informatikai eszközöket csak a Társaság arra felhatalmazott munkavállalói használhatják, a mobil eszközök használatának helyét az eszközök eszköznyilvántartása rögzíti.
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.
A használni kívánt adathordozót (pendrive, külső HDD) a tárolásra kijelölt helyről kell kivenni, és oda is kell visszahelyezni. A munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek.
Adathordozót másnak átadni csak engedéllyel szabad. A munkák befejeztével a használt berendezést, eszközt és környezetét rendbe kell tenni.

11.3. Vírusvédelem

Vírusfertőzés gyanús helyzetek

- A víruskereső program névvel azonosított vírust jelez.
- Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő.
- Szokatlan és váratlan képernyő-tevékenység (szokatlan üzenetek, ablakok megjelenése).
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak).
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál.

Gyanús helyzet észlelésekor haladéktalanul értesíteni kell a rendszergazdát.

Vírusvédelmi teendők

Az alábbi utasítások betartása erősen ajánlott a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében:

- Vírusvédelmi szoftverrel biztosítani kell a munkaállomások vírusvédelmét. Ehhez a Társaság az ESET vírusvédelmi szoftvert alkalmazza.
- A vírusvédelmi programnak rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik és állandó háttérvédelmet biztosít. A felhasználóknak nem szabad kikapcsolni ezt a védelmet.
- Nem futhat egyszerre két vírusölő program.
- Havonta minden gépen teljes vírusellenőrzést kell végrehajtani (a vírusvédelmi szoftver támogatja az időzített keresési funkciót).
- A vírusvédelmi program vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell. Ha erre lehetőség van, az automatikus frissítést kell választani, így az új elemek rögtön megjelenésük után felkerülhetnek a rendszerre.
- Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.
- Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mailek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket. Az e-mailben küldött vírusok rendszeresen operálnak valamilyen különös megjegyzéssel a levél tárgya mezőben.

Teendők vírusfertőzés esetén

- Tájékoztatni kell a rendszergazdákat a fertőzésről vagy annak gyanújáról, akik az alábbiakban részletezett eljárást követik.
- A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó hordozóról. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).
- A vírusvédelmi szoftvert elindítják, és megszüntetik a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.

- A víruskeresést addig kell végezni, amíg el nem éri a rendszergazda, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál.

11.4. Levelezést érintők kérdések

Általános érvényű szabályok

A Társaság minden alkalmazottjának kötelező <felhasznalonev>@prosperisalba.hu formájú postafiókot használni, amit a rendszergazda ad belépéskor. A Társaság nem monitorozza a hálózatából küldött, illetve ide érkező levelek tartalmát.

A Társaság hálózatán átmenő leveleken központilag vírusellenőrzés történik, ami különböző védelmi és szűrési funkciókkal egészül ki.

A SPAM-ek miatt a Társaság kétlépcsős biztonsági rendszert vezetett be. Első lépcsőben egy spamszűrő szerverre érkeznek be a levelek (mailgw.oik.co.hu), ahol a beérkezett levelek szűrése után érkeznek a Társaság levelezőszerverére. Ott a cPanel szoftver SpamAssassin levélszemétszűrője is átvizsgálja a leveleket, amik ezután érkeznek meg a postaládákba. Ezek a folyamatok időbeni kiesést nem okoznak a levélforgalomban.

Alapelvek

- A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartásformát.
- A levelek tartalma nem sérthet meg szerzői és kapcsolódó jogokat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.
- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése, illetve továbbküldése.
- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről a Társasági levelező rendszert e-mail szeméttel (SPAM) terhelhetik meg.
- A Társaság hálózatán maximum 50 Mb méretű levelek küldhetők, ez a korlát az egyes helyi szerverek levelező rendszerei esetében pozitív irányban módosulhat.
- A felhasználó postafiókja maximum 50 GB. Indokolt esetben ennek mérete eltérhet, megváltoztatásához ügyvezetői engedély szükséges. A felhasználó köteles gondoskodni arról, hogy ezt a korlátot ne lépje túl (régi, nem fontos, nagyméretű levelek törlése, törölt levelek végleges eltávolítása, elküldött levelek törlése).

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 bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- a még használható anyag(ok) mentése,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával a feldolgozás folytatása.

Szerverek esetében a megfelelő védelmet az ÖIK biztosítja.

12.2. Hardvervédelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetést, karbantartást és szervizelést az ÖIK végzi.
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

a) adatbevitel hibátlan műszaki állapotú berendezésen történjen;
b) tesztelt adathordozóra lehet adatállományt rögzíteni;
c) a bizonylatokat és adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani;
d) az adatrögzítő szoftver védelme: lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is;
e) 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 munkaállomások rendszergazdai jelszavát a Társaság Ügyvezetője, a szerverek rendszergazdai jelszavát az ÖIK 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 adathordozók a Társaság tárgyi eszköz leltárában kerülnek nyilvántartásra.

12.3.3. Adathordozók tárolása

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

12.3.4. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a hatályos jogszabályokban meghatározott bizonylatőrzési kötelezettségnek megfelelően kell meghatározni.

12.3.5. Selejtezés, sokszorosítás, másolás

A selejtezést a Társaság selejtezési szabályzata alapján kell lefolytatni.
Sokszorosítás, másolás kizárólag a Társaságnál érvényben lévő belső utasítások szerint végezhető. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

12.3.6. Leltározás

A szoftvereket és adathordozókat a Társaság leltározási szabályzatában foglaltaknak megfelelően kell leltározni.

12.3.7. Mentések, fájlok 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 ÖIK segítséget nyújt.
A szervereken tárolt adatokról a biztonsági mentést rendszeres időközönként el kell végezni, amelyért az ÖIK felelős.

12.4. Szoftvervédelem

12.4.1. Rendszerszoftver védelem

Az ÖIK feladata biztosítani, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

12.4.2. Felhasználói programok védelme

a) 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.

b) Programok megőrzése, nyilvántartása
   A programokról a Társaság naprakész nyilvántartást köteles vezetni.
   A számvitelről szóló 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 a Társaság ügyvezetője, a programok működőképes állapotban való tartásáért az ÖIK felelős.

13. A hálózat munkaállomásainak működésbiztonsága

Külső helyről hozott vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az ÖIK-et azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell a működésüket.
A Társaság informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül tilos.
A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
A Társaság tulajdonában, vagy üzemeltetésében lévő informatikai eszközt és tartozékait a helyéről elvinni csak a Társaság ügyvezetőjének engedélyével szabad.

13.1. Jelszókezeléssel kapcsolatos szabályok

A felhasználók a Társaság által biztosított eszközön használt jelszavukat 3 havonta kötelesek cserélni.
A jelszónak minden felhasználó által bármikor megváltoztathatónak kell lennie. A kezdetben generált jelszót az első bejelentkezés alkalmával meg kell változtatni.
A jelszó minimum 12 karakter hosszú legyen, és tartalmazzon (kicsi és nagy) betűket és számjegyeket is. További feltétel, hogy nem tartalmazhatja a felhasználó nevét még részleteiben sem.

A jelszó nem írható fel semmilyen jól látható vagy könnyen hozzáférhető helyre. A jelszavakat nem szabad felírni, papíron tárolni, amennyiben az elkerülhetetlen (pl. kezdetben generált jelszó esetén) gondoskodni kell a jelszó biztonságos helyen, zárt borítékban történő tárolásáról.
A jelszó és a hozzátartozó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezés során sem.
Ha a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie.

14. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során az Informatikai Biztonsági Szabályzat rendelkezéseinek betartását a Társaság ügyvezetője ellenőrzi.

15. Záró rendelkezések

A Társaság 2026. március 20. napjától hatályos Informatikai Biztonsági Szabályzata 2026. április 30. napjával hatályát veszti.

A jelen szabályzatban foglaltak 2026. május 1. napjától hatályosak.

Székesfehérvár, 2026. 04. 23.

Pálóczy Renáta
ügyvezető