# INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

## Nagyszentjánosi Közös Önkormányzati Hivatal

Hatályos: 2019. július 1-jétől

A Szabályzatot jóváhagyta:
Nagyszentjános Község Képviselő-testülete a 69/2019. (IV. 23.) sz. határozatával
Rétalap Község Képviselő-testülete a 37/2019. (V. 15.) sz. határozatával

Németh Dániel
jegyző

Nagyszentjánosi Közös Önkormányzati Hivatal jegyzője

# Tartalomjegyzék

# INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

## Jogszabályi környezet

> Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
> 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
> 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről
> 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

## 1. Az Informatikai Biztonsági Szabályzat célja

A Nagyszentjánosi Közös Önkormányzati Hivatal Jegyzője a Nagyszentjánosi Közös Önkormányzati Hivatal részére az elektronikus információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatokat az alábbi szabályzat szerint határozza meg.

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 üzembe helyezésen 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 a Nagyszentjánosi Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) alkalmazottjaira, függetlenül attól, hogy alkalmazására milyen jogviszonyban kerül sor.

### 2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed a Hivatal tulajdonában lévő, illetve az általa használt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- 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

*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, illetőleg 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

A Hivatal adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a Hivatal 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 mindenkori rendszergazda.
A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Hivatal vezetőinek kell gondoskodnia.

### 7.1. Adatvédelmi felelősök feladatai

*a) Informatikai vezető feladatai:*

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi feladatok ismertetése,
- 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, (4.sz. melléklet)
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a Hivatal informatikai rendszer hardver eszközeinek karbantartásáért,
- 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,

7.2. **Az informatikai vezető 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. Az informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet,
- 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.

## 8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezető és a rendszergazda oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
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 az informatikában - valamint a Hivatalnál - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása a Hivatal feladata.

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

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

I. — közlésre szánt, bárki által megismerhető adatok,
II. — minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője a Hivatal vezetője.
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 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 biztosítani kell (szoftver, hardver adatvédelem). Ennek biztosítása a rendszergazda feladata.

# 9. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, mert ezen helyzetekből adódó adatvesztésért a rendszert felügyelő személy nem tud felelősséget vállalni.

## 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, melyekért a rendszert felügyelő személy nem tud felelősséget vállalni

*Szándékos károkozás..*

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

*Nem szándékos, illetve gondatlan károkozás:*

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a 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 IBSZ nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartását.

### 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 Hivatal arra felhatalmazott alkalmazottai 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, ennek felelőssége a Hivatalt terheli
- a használni kívánt adathordozót 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

A Hivatal Tűzvédelmi Szabályzata szerint.

# 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 a rendszergazda végzi.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak a rendszergazda 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.
- Az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

*12.3.2. Adathordozók tárolása*

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani (7.1.-es pontban rögzített módon)

*12.3.3. Az adathordozók megőrzése*

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

*12.3.4. Selejtezés, sokszorosítás, másolás*

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

*12.3.5. Leltározás*

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

*12.3.6. Mentések, file-ok védelme*

Az adatfeldolgozás után biztosítani kell az adatok mentését (7.1-es pontban rögzítve)
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 rendszergazdának kell készítenie. Az archiválásban a rendszergazda segítséget nyújt.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda a felelős.

**12.4. Szoftver védelem**

*12.4.1. Rendszerszoftver védelem*

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára. A szoftverek vírusmentesítését a rendszergazda a Hivatal által használatos antivírus szoftverrel látja el.

*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.
Az adatállományokhoz való hozzáféréshez szükséges van jelszóval ellátott védelemre, a jelszó nem lehet 6 karakternél rövidebb, tartalmaznia kell kis-, ill. nagybetűt, legalább egy karaktert és legalább egy számot. A jelszavak nyilvántartása és tárolása a Hivatal felelőssége.

*Programok megőrzése, nyilvántartása*

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni
A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a Hivataloknak 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. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

## 13.1. Központi gép

Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
A központi gép háttértárairól folyamatosan biztonsági mentést kell készíteni.
Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.
A vásárolt szoftverekről biztonsági másolatot kell készíteni.

## 13.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés, gyanúja esetén az informatikusokat azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A Hivatal informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső

felhasználói igények kielégítésein kívül nem szabad.
A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

## 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 IBSZ rendelkezéseinek betartását a Hivatal vezető ellenőrzi.

## 15. Záró rendelkezések

Az Informatikai Biztonsági Szabályzat 2019. július 1-jén lép hatályba, és hatálybalépésével a tárgykörben kiadott szabályzatok hatályukat vesztik.

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

Az érintett dolgozók a szabályzatban foglaltak megismerését a megismerési nyilatkozat aláírásával tanúsítják.

Nagyszentjános, 2019. április 1.

Németh Dániel
jegyző

# 1. sz. melléklet

# a Nagyszentjánosi Közös Önkormányzati Hivatal biztonsági osztályba sorolása

# a 77/2013. (XII. 19.) NFM rendelet 1. számú melléklete alapján

*Az elektronikus információs rendszerek biztonsági osztályba sorolása*

**1. Általános irányelvek**

1.1. Az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesíti, így például

1.1.1. a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;

1.1.2. a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;

1.1.3. a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását kockázatelemzés alapján kell elvégezni, amit az érintett szervezet vezetője hagy jóvá. A kockázatelemzés során ajánlott a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevétele.

1.2.1. Az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemezés alapját

1.2.1,1. az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, és az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának

sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága;

1.2.1.2. a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége

képezi.

1.3. A biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.

1.4. Az elektronikus információs rendszerek biztonsági osztályai meghatározásához az alábbi - az érintett szervezetnél szóba jöhető - közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell - az érintett szervezet jellemzőire tekintettel - Figyelembe venni:

1.4.1. társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat (így pl. alaptevékenységek akadályozása, különösen a létfontosságú információs rendszerelemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal,

felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);
1.4.2. személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének - ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet - veszélye);
1.4.3. közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);
1.4.4. közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).
1.5. A veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.

**2. Biztonsági osztályok**
Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: tv.) szerint a besorolás elvégzése a következő elvek figyelembevételével az érintett szervezet felelőssége, az alábbiak a döntéshez csak szempontokat jelentenek:

A Nagyszentjánosi Közös Önkormányzati Hivatal biztonsági osztályba sorolási szintje: **2. biztonsági osztály**
A 2. biztonsági osztály esetében **csekély káresemény következhet** be, mivel
személyes adat sérülhet;

- az üzlet-, vagy ügymenet szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

# 2. sz. melléklet
# a 77/2013. (XII. 19.) NFM rendelet 2. melléklete alapján

**Az elektronikus információs rendszereket működtető szervezetek** biztonsági szintbe sorolása

## 1. Általános irányelvek

1.1. Az érintett szervezet biztonsági szintjét meghatározza a működtetett elektronikus információs rendszerek biztonsági osztályba sorolása. Az érintett szervezet a biztonsági szintbe soroláskor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a szervezet feladataira, a vele szemben fennálló elvárásokra tekintettel, és a kockázatokhoz illeszkedő súllyal érvényesíti. A legmagasabb biztonsági osztályba sorolt rendszer biztonsági osztályát ennek figyelembevételével lehet a biztonsági szint meghatározásakor mérvadónak, vagy nem mérvadónak tekinteni.

1.2. Az egyes biztonsági szinteknek fokozatosan szigorodó biztonsági jellemzői vannak. Az egyes szintekbe történő besorolás egyben a további kockázatelemzés egyik alapja is.

## 2. A biztonsági szintek

2.2. **Az érintett szervezet biztonsági szintje 2.,** ha az érintett szervezet által működtetett elektronikus információs rendszerek esetén nincs 2. biztonsági osztálynál magasabb besorolású rendszer, és az érintett szervezet elfogadja, hogy az érintett szervezet informatikai folyamatai részben szabályozottak, azaz:

2.2.1. az érintett szervezetnél a biztonsági folyamatoknak nincsenek részletszabályai, azokat az elfogadott magas szintű szabályzatok (informatikai biztonságpolitika, informatikai biztonsági stratégia, informatikai biztonsági szabályzat, valamint a tervezésre, beszerzésre, fejlesztésre, képzésre vonatkozó szakterületi belső előírások) szabályozzák;

2.2.2. az elektronikus információs rendszerek biztonságához kapcsolódó eljárások kialakítására törekednek, de ehhez sem megfelelő szaktudás, sem megfelelő eszközrendszer nem áll rendelkezésre;

2.2.3. az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket és feladatokat egy, az elektronikus információs rendszer biztonságáért felelős, irányítási jogkörében korlátozott személyhez rendelték hozzá;

2.2.4. az elektronikus információs rendszerek előállítanak a biztonságra vonatkozó információkat, de azokat a szervezet nem elemzi;

2.2.5. az elektronikus információs rendszerek biztonságára vonatkozó jelentések nem teljes körűek;

2.2.6. az elektronikus információs rendszerek biztonságát nem az érintett szervezet teljes körű biztonságának részeként, hanem elsősorban az informatika belső felelősségeként, területeként kezelik;

2.2.7. a fizikai beléptetés ellenőrzésén túlmenően a működtetett rendszer és a kezelt adatok védelme további fizikai védelmi intézkedéseket nem igényel.

# 3. sz. melléklet

# A Szabályzat 7. pontjához:

## A védelem felelősei

1. Informatikai vezető: a Hivatal vezetője

2. A vezető által megbízott végrehajtó a Hivatal által szerződéssel megbízott mindenkori rendszergazda

# 4. sz. melléklet

# A biztonsági mentések hozzáférései

A biztonsági mentés a következő képen zajlik:

1) a felhasználó a személyi számítógépén létrehozza a dokumentumot

2) a létrehozott dokumentum egy másolata felkerül a központi adatmentő egységre, mely RAID1-es módszerrel tükrözi a felkerült adatot.

3) A központi adatmentő egységből egy külső merevlemezre kerül az adatok másolata.

4) A külső adatmentő egység elzárásra kerül a Hivatal által meghatározott helyen.

5) A biztonsági mentések hozzáféréséhez szükséges jelszavak tárolásáért a Hivatal vezetője a felelős.