

# **Csetényi Közös Önkormányzati Hivatal**

## **INFORMATIKAI BIZTONSÁGI SZABÁLYZATA**

### **1. Az Informatikai Biztonsági Szabályzat ( IBSZ ) 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 működni 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 Csetényi Közös Önkormányzati Hivatallal jogviszonyban álló munkavállalóira.

#### ***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 bérelt 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, előírászerű 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 informatikus ( megbízási szerződéssel ).

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a hivatal vezetőinek kell gondoskodnia.

### **7.1. Adatvédelmi felelős feladatai**

a) Informatikus feladatai:

- 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

### **7.2. A hivatal 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. A hivatal vezető jogai**

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a vállalkozás vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthez 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 dolgozóknak 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 vezető feladata.

### **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 hivatal vezetőjének jelenteni kell.

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,
- feszültség-ingadozás,
- 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 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***

- a termék külső és belső helyiségeit biztonsági zárral kell felszerelni,
- a terembe való be- és kilépés rendjét szabályozni kell,

### ***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 (DVD, 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***

A terem illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

A vállalkozás géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.

A vállalkozás géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

## **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, háttértákról 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 bevitelénél alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető 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 hivatal selejtezésének szabályzata alapján kell lefolytatni. Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítását 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 rendszergazdák 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 hozzáférhetőek 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. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága**

#### **13.1. Központi gépek**

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

A központi gépek háttértáiról 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 vállalkozás 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 az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

## **15. Záró rendelkezések**

**Az Informatikai Biztonsági Szabályzat 2014. február 1 - én lép hatályba.**

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

**Csetény, 2014. január 31.**

**Müller József  
jegyző**