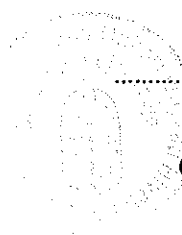
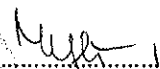


**BALATONKERESZTÚRI KÖZÖS  
ÖNKORMÁNYZATI HIVATAL**

**INFORMATIKAI BIZTONSÁGI SZABÁLYZATA**

Jóváhagyta, kiadta:



  
.....  
**Mestyán Valéria**  
**Címzetes Főjegyző**

Érvénybe lépett : 2018.01.01.

**BELSŐ HASZNÁLATRA !**

## Tartalomjegyzék

I. Általános irányelvek	5.
I.1. IBSZ célja	5.
I.2. Az IBSZ hatálya	6.
I.3. Az IBSZ módosítása, felülvizsgálata	7.
I.4. Kapcsolódó szabályzatok	7.
I.5. Az Informatikai Biztonsági Szabályzat alkalmazásának módja	7.
I.6. Az elektronikus információs rendszer biztonsági osztályba sorolása	7.
I.7. A Közös Hivatal biztonsági szintje	8.
II. Védelmi intézkedés katalógus	8.
II.1. Adminisztratív védelmi intézkedések	8.
II.1.1.1. Szervezeti szintű alapfeladatok	8.
II.1.1.1	8.
II.1.1.2.	8.
II.1.1.3. Informatikai biztonsági szabályzat	9.
II.1.1.4. Az elektronikus információs rendszerek biztonságáért felelős személy	9.
II.1.1.5. Pénzügyi erőforrások biztosítása	9.
II.1.1.6. Az intézkedési terv és mérőföldkövei	9.
II.1.1.7. Az elektronikus információs rendszerek nyilvántartása	10.
II.1.1.8.	10.
II.1.1.9. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	10.
II.1.2. Kockázatelemzés	11.
II.1.2.1. Kockázatelemzési eljárásrend	11.
II.1.2.2. Biztonsági osztályba sorolás	11.
II.1.2.3. Kockázatelemzés	11.
II.1.3. Tervezés	11.
II. 1.3.1. Biztonságtervezési eljárásrend	11.
II. 1.3.2. Rendszerbiztonsági terv	11.
II. 1.3.3. Személyi biztonság	11.
II. 1.3.4. Viselkedési szabályok az interneten	15.
II. 1.4. Rendszer és szolgáltatás beszerzés	15.
II. 1.4.1. Beszerzési eljárásrend	15.
II. 1.4.2. A rendszer fejlesztési életciklusa	15.
II. 1.4.3. Külső elektronikus információs rendszerek szolgáltatásai	16.
II.1.5. Emberi tényezőket figyelembe vevő – személy – biztonság	15.
II.1.5.1. Eljárás a jogviszony megszűnésekor	15.
II.1.5.2. Fegyelmi intézkedések	16.
II.1.6. Tudatosság és képzés	16.
II.1.6.1. Képzési eljárásrend	16.
II.1.6.2. Biztonság tudatosság képzés	17.
II.1.6.3. Belső fenyegetés	17.
II.2. Fizikai védelmi intézkedések	18.

II.2.1. Fizikai és környezeti védelem	18.
II.2.1.1. Fizikai védelmi eljárásrend	18.
II.2.1.2. Fizikai belépési engedélyek	19.
II.2.1.3. A fizikai belépés ellenőrzése	19.
II.3. Logikai védelmi intézkedések	19.
II.3.1. Konfigurációkezelés	19.
II.3.1.1. Konfigurációkezelési eljárásrend	19.
II.3.1.2. Alapkonfiguráció	20.
II.3.1.3. Elektronikus információs rendszerelem leltár	20.
II.3.1.4. A szoftverhasználat korlátozásai	20.
II.3.1.5. A felhasználó által telepített szoftverek	20.
II.3.2.1. Ügymenet folytonosság tervezése	20.
II.3.2.1. Ügymenet folytonosságra vonatkozó eljárásrend	21.
II.3.2.2. Ügymenet folytonossági terv informatikai erőforrás kiesésekre	21.
II.3.2.3. Az elektronikus információs rendszer mentései	21.
II.3.3. Karbantartás	22.
II.3.3.1. Rendszer karbantartási eljárásrend	22.
II.3.3.2. Rendszeres karbantartás	22.
II.3.4. Adathordozók védelme	22.
II.3.4.1. Adathordozók védelmére vonatkozó eljárásrend	22.
II.3.4.2. Hozzáférés az adathordozókhoz	22.
II.3.4.3. Adathordozók törlése	23.
II.3.4.4. Adathordozók használata	23.
II.3.5. Azonosítás és hitelesítés	23.
II.3.5.1. Azonosítási és hitelesítési eljárásrend	23.
II.3.5.2. Azonosítás és hitelesítés	23.
II.3.5.3. Azonosító kezelés	23.
II.3.5.4. A hitelesítésre szolgáló eszközök kezelése	24.
II.3.5.5. A hitelesítésre szolgáló eszköz visszacsatolása	24.
II.3.5.6. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	24.
II.3.5.7. Hitelesítés szolgáltatók tanúsítványának elfogadása	24.
II.3.6. Hozzáférés ellenőrzése	25.
II.3.6.1. Hozzáférés ellenőrzési eljárásrend	25.
II.3.6.2. Felhasználói fiókok kezelése	25.
II.3.6.3. Hozzáférés ellenőrzés érvényesítése	25.
II.3.6.4. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	26.
II.3.6.5. Külső elektronikus információs rendszerek használata	26.
II.3.6.6. Nyilvánosan elérhető tartalom	26.
II.3.7. Rendszer- és információsértetlenség	26.
II.3.7.1. Kártékony kódok elleni védelem	26.
II.3.7.2. Az elektronikus információs rendszer felügyelete	26.
II.3.7.3. A kimeneti információ kezelése és megőrzése	27.
II.3.8. Naplózás és elszámoltathatóság	27.

II.3.8.1. Naplózási eljárásrend	27.
II.3.8.2. Naplózható események	27.
II.3.8.3. Naplóbejegyzések tartalma	27.
II.3.8.8. Időbélyegek	27.
II.3.8.9. A naplóinformációk védelme	28.
II.3.8.11. A naplóbejegyzések megőrzése	28.
II.3.8.12. Naplógenerálás	28.
II.3.9. Rendszer- és kommunikációvédelem	28.
II.3.9.1. Rendszer- és kommunikációvédelmi eljárásrend	28.
II.3.9.2. A határok védelme	28.
II.3.9.3. Kriptográfiával kapcsolatos szabályozás	29.
II.3.9.4. Együttműködésen alapuló számítástechnikai eszközök	29.
II.3.9.5 A folyamatok elkülönítése	29.
III. Jogszabály hivatkozás	31.
IV. Értelmező rendelkezések	32.
V. Mellékletek	36.
V.1. számú melléklet, -IBSZ hatálya alá tartozó költségvetési szervek	36.
V.2. számú melléklet, -Az információs rendszer biztonsági osztályba sorolása	36.
V.3.számú melléklet, - A Közös Hivatal biztonsági szintje	39
V.4. számú melléklet, -Kockázatelemzési és kezelési módszertan	40.
V.5. számú melléklet, -Hozzáférés jogosultság igénylő lap	44.
V.6. számú melléklet, -Hozzáférés jogosultság igénylő lapok összesítése	45.
V.7. számú melléklet, - Biztonsági események jelentése	46.
V.8. számú melléklet, -Megismerési nyilatkozat	48.
V.9. számú melléklet, - Az Önkormányzat weboldala	49.
V.10. számú melléklet, - Polgármesteri megismerési nyilatkozat	50.

# **Balatonkeresztúri Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata**

A Balatonkeresztúri Közös Önkormányzati Hivatal 8648 Balatonkeresztúr Ady E. u. 52. (továbbiakban: Hivatal) Informatikai Biztonsági Szabályzata (továbbiakban: IBSZ), mely az informatikai rendszerrel kapcsolatos adatvédelem és adatbiztonság megteremtése érdekében – helyi önkormányzatokról szóló 2011. évi CLXXXIX. ASP bevezetésével foglalkozó törvény, az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvényben, és az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI. 22.) KSH rendelkezésben foglaltak, valamint a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információ biztonságáról (továbbiakban: Törvény), és a 41/2015. (VII. 15.) BM rendelet (továbbiakban: Rendelet) figyelembe vételével – készült.

## **I. Általános irányelvek**

### **I.1. Az IBSZ célja**

Az IBSZ alapvető célja olyan szabályok megfogalmazása, melyek alapján az elektronikus információs rendszer teljes életciklusában biztosítja az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az informatikai rendszerek és környezetük fizikai, logikai és adminisztratív védelmi követelményei alapján, megfogalmazni a védelmi rendszerek továbbfejlesztéséhez, illetve megvalósításához szükséges teendőket, a követelményeknek megfelelő eredményes és hatékony működés biztosítása érdekében.

#### **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,

- adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- adatállományok tartalmi és formai épségének megőrzése,
- 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.

## **I.2. Az IBSZ hatálya**

### **Szervezeti – személyi hatály**

Az IBSZ hatálya kiterjed a Hivatal valamennyi szervezeti egységére, mindazon személyekre, akik munkájuk végzése során vagy egyéb céllal a „Tárgyi hatály” pontban meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat hoznak létre, tárolnak, felhasználnak, vagy továbbítanak, illetve azokra, akik ezen tevékenységekkel kapcsolatosan döntéseket hoznak. ( 1.sz. melléklet)

Ezen személyek körébe tartoznak:

- polgármester, alpolgármester, főjegyző, képviselők,
- jogviszony alapján foglalkoztatott munkavállalókra,
- a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre,

### **Tárgyi hatály**

Az IBSZ hatálya kiterjed aHivatal bármely szervezeti egysége által használt (vásárolt vagy bérelt) illetve üzemeltetett informatikai eszközre és berendezésre, amely tárolja, kezeli, feldolgozza, felügyeli, ellenőrzi és továbbítja az Hivatal kezelésében lévő adatokat, információkat;

A Hivatal területén bármely okból használt, más személy vagy szervezet tulajdonát képező informatikai eszközre és berendezésre.

### **Területi hatály**

Az IBSZ hatálya kiterjed a Balatonkeresztúri Közös ÖnkormányzatiHivatalt fenntartó önkormányzatokra, valamint azok intézményeire is.( Balatonberény Község Önkormányzata, 8649, Kossuth tér 1.,Balatonmáriafürdő Község Önkormányzata 8647, Gróf Széchenyi Imre

tér 9.)Ezen belül mindazon helyiségekre, amelyekben a „Tárgyi hatály” pontban meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat hoznak létre, tárolnak, felhasználnak, vagy továbbítanak.

#### **Időbeli hatály**

Az IBSZ a hatályba lépés napjától a visszavonásig érvényes.

#### **További hatály**

Az IBSZ hatálya kiterjed a fenti pontokban felsorolt területekkel kapcsolatos szabályozásokra és utasításokra. Ennek megfelelően az IBSZ-el ellentétes szabályozás illetve utasítás a Hivatalnál nem léphet hatályba.

#### **Hatásköri és illetékességi szabályok**

Az IBSZ belső használatú dokumentum. A Jegyző feladata az IBSZ megismertetése az érintettekkel, illetve a benne foglalt információk védelme az illetéktelenek ellen.

### **I.3. Az IBSZ módosítása, felülvizsgálata**

Az IBSZ eseti módosítására akkor kerül sor, ha a benne szereplő adatok megváltoztak, illetve ha az IBSZ olyan kisebb mértékű kiegészítésekre szorul, amelyek nem érintik az aktuális biztonsági követelményeket.

Az IBSZ módosítására van szükség, ha a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be vagy a Hivatal elektronikus információs rendszereinek üzemeltetésével kapcsolatban változások történnek.

Az IBSZ-t legalább évente egy alkalommal felül kell vizsgálni.

Az IBSZ eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a jegyző hatásköre.

### **I.4. Kapcsolódó szabályzatok**

Az IBSZ előírásai összhangban vannak az Hivatal alábbi dokumentumaival:

Pénz és értékezelési szabályzat

Számviteli politika

Tűzvédelmi szabályzat

SZMSZ, munkaköri leírások

Iratkezelési szabályzat

Információ átadási szabályzat

### **I.5. Az Informatikai Biztonsági Szabályzat alkalmazásának módja**

Az IBSZ megismerését az érintett dolgozók részére a Jegyző és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kell vezetni.

Az IBSZ alapján a munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

### **I.6. Az elektronikus információs rendszer biztonsági osztályba sorolás**

A 2. biztonsági osztály esetében csekély káresemény bekövetkeztével kell számolni.

Személyes adat sérülhet, az ügymenet szempontjából csekély értékű, és csak belső szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet. A lehetséges társadalmi-politikai hatás a Hivatalon belül kezelhető. A közvetlen és közvetett anyagi kár a Hivatal költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

A Hivatal a Törvényben, valamint a Rendeletben szabályozottak szerint elvégezte a működtetett elektronikus információs rendszerek, és a bennük kezelt adatok - bizalmasság, sértetlenség, rendelkezésre állás elvek alapján - biztonsági osztályba sorolását (2.számú melléklet- Az információs rendszer biztonsági osztályba sorolása).

**Az elektronikus információs rendszerek biztonsági osztálya: 2 szintű.**

### **I.7. A Hivatal biztonsági szintje**

**Az elvárt biztonsági szintje: 2**

I. Ahhoz, hogy a hivatal a 2. biztonsági osztály részére támasztott követelményeknek megfeleljen, az alábbi szabályokat kell betartani.

#### **II. Védelmi intézkedés katalógus**

##### **II.1. Adminisztratív biztonsági intézkedések**

###### **II.1.1. Szervezeti szintű alapfeladatok**

II.1.1.1 törölve.

II.1.1.2 törölve.

###### **II.1.1.3. Informatikai biztonsági szabályzat**



A jelen szabályzat amely, az érvényes követelmények szerint tartalmazza mindazon szabályok összességét, melyek biztosítják az informatikai biztonsági megteremtését. Az IBSZ-ről minden érintettet tájékoztatni kell. Az informatikai biztonsági szabályzat tartalmazza:

- az információbiztonság szervezetrendszerének belső együttműködését,
- biztonsági osztályba és biztonsági szintbe sorolást,
- kockázatelemzést
- mindazon elvárásokat, amelyeket a vonatkozó jogszabályok a Hivatalra vonatkozóan meghatároznak.

#### **II.1.1.4. Az elektronikus információs rendszerek biztonságáért felelős személy**

A Jegyző – a Törvényben meghatározott követelmények alapján - kinevez, vagy megbíz az elektronikus információs rendszer biztonságáért felelős személyt (továbbiakban: IBF).

Az IBF ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló Törvényben meghatározott feladatokat (részletezés a II. fejezet 1.3.3 pontban).

#### **II.1.1.5. Pénzügyi erőforrások biztosítása**

A Hivatal a költségvetési határozatában megtervezi az informatikai biztonsági stratégia megvalósításához szükséges forrásokat, amit a fenntartó önkormányzatok biztosítanak.

Intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásának biztosításáról.

#### **II.1.1.6. Az intézkedési terv és mérföldkövei**

A Hivatal intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához, és ebben mérföldköveket határoz mely alapján meghatározott időnként felülvizsgálja és karbantartja az intézkedési tervet a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján.

Amennyiben az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál hiányosság állapítható meg, a vizsgálatot követő 90 napon belül a cselekvési tervet kell készíteni, a hiányosság megszüntetésére. Felelős a Jegyző és az IBF.

#### **II.1.1.7. Az elektronikus információs rendszerek nyilvántartása**

A Hivatal (6.számú melléklet, Elektronikus rendszerelem leltár) folyamatosan vezetett nyilvántartást készít az elektronikus információs rendszereiről. A nyilvántartás minden rendszerre nézve tartalmazza:

- annak alapfeladatait, valamint a rendszerek által biztosítandó szolgáltatásokat,
- a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait,
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait.

A fentiek betartásáért a **Jegyző a felelős.**

#### **II.1.1.8. törölve**

#### **II.1.1.9. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás**

Új eszközök használatba vételét a Jegyző engedélyezi. Az SZMSZ-ben, a munkaköri leírásokban, az IBSZ-ben rögzíteni kell, az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési **eljárási folyamatokat**. Meg kell határozni az információbiztonsággal összefüggő **szerepköröket** és az ezeket betöltő **személyeket** (5. számú melléklet, - Hozzáférés jogosultság igénylő lapok összesítése). Integrálni kell az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba.

### **II.1.2. Kockázatelemzés**

#### **II.1.2.1. Kockázatelemzési eljárásrend**

A Hivatal megfogalmazza a kockázatelemzési eljárásrendet, mely az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő, valamint meghatározza ennek gyakoriságát.

#### **II.1.2.2. Biztonsági osztályba sorolás**

A Hivatal által használt elektronikus információs rendszereket - bizalmassága, sértetlensége és rendelkezésre állása szempontjából - a Törvény legalább a 2-es biztonsági osztályba sorolja.

Az IBF a jogszabályban meghatározott szempontok alapján előkészíti, a Jegyző jóváhagyja, az elektronikus információs rendszerek biztonsági osztályba sorolásának eredményét. A

biztonsági osztályba sorolás eredményét jelen szabályzat 1.számú mellékletben - Az információs rendszer biztonsági osztályba sorolása - található.

A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételt el kell készíteni.

### **II.1. 2.3. Kockázatelemzés**

A Jegyző végrehajtja a biztonsági kockázatelemzéseket és annak eredményét rögzíti jelen szabályzatban (3.számú melléklet, - Kockázatelemzési és kezelési módszertan).

A Jegyző felülvizsgálja a kockázatelemzések eredményét és tájékoztatja az érintetteket erről. Meg kell ismételni a kockázatelemzést, ha változás áll be az elektronikus információs rendszerben, annak biztonságát befolyásoló egyes körülmények felmerülésekor vagy annak működési környezetében. Az rendszer felhasználóival és egyéb érintettekkel ismerteti a kockázatelemzés eredményét. A kockázatelemzés eredményei, annak részletei jogosulatlanok számára nem ismerhetők meg.

### **II.1.3. Tervezés**

#### **II.1.3.1. Biztonságtervezési eljárásrend**

A Jegyző a jelen szabályzatban, és az SZMSZ-ben, valamint a munka- és feladatkörük miatt érintettek számára a munkaköri leírásokban definiálja a biztonságtervezési eljárásnak megfelelő elvárásokat, szabályokat.

#### **II.1.3.2. Rendszerbiztonsági terv**

A Hivatal, amennyiben az elektronikus információs rendszert *tervez vagy fejleszt, előzetesen* rendszerbiztonsági tervet készít. A rendszerbiztonsági tervet a Rendeletben meghatározottak szerint kell elkészíteni.

A Hivatal saját fejlesztésű alkalmazást, szoftvert nem használ, *elektronikus információs rendszert nem tervez, nem fejleszt.*

#### **II.1.3.3. Személyi biztonság**

##### **A Jegyző**

- **biztosítja** az elektronikus információs rendszerre irányadó **biztonsági osztály** tekintetében a jogszabályban meghatározott **követelmények teljesülését**,
- **biztosítja** a szervezetre irányadó **biztonsági szint** tekintetében a jogszabályban meghatározott követelmények teljesülését,
- az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer **biztonságáért felelős személyt nevez ki** vagy bíz meg,

- **meghatározza** a szervezet elektronikus információs rendszerei védelmének **felelőseire, feladataira** és az ehhez szükséges **hatáskörökre**, felhasználókra vonatkozó **szabályokat**, illetve kiadja az **informatikai biztonsági szabályzatot**,
- gondoskodik arról, hogy az elektronikus rendszerhez való **hozzáférés engedélyezését** írásbeli nyilatkozattétel előzze meg (4.számú melléklet, - Hozzáférési jogosultság igénylő lap),
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek **oktatásáról**, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
- rendszeresen végrehajtott biztonsági **kockázatelemzések**, ellenőrzések, lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
- gondoskodik az elektronikus információs rendszer eseményeinek **nyomon követhetőségéről**,
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő **gyors és hatékony reagálásról**, és ezt követően a biztonsági események kezeléséről,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak **szereződéses kötelemként** teljesüljenek,
- ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan **tájékoztatásáért**,
- megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
- **A fentiekben** meghatározott feladatokért a Jegyző abban az esetben is felelős ha az üzemeltetéshez, adat feldolgozáshoz közreműködőt vesz igénybe, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.
- A Jegyző köteles **együttműködni a hatósággal**.

**Az elektronikus információs rendszer biztonságáért felelős személy ( IBF )**

- Feladata ellátása során joga van a szervezet vezetőjének közvetlenül tájékoztatást, jelentést adni.
- Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:
- gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- elvégzi vagy irányítja az előbbiektől tevékenységek **tervezését, szervezését, koordinálását és ellenőrzését,**
- **előkészíti** a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- **előkészíti** a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- **véleményezi** az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal,
- az elektronikus információs rendszert érintő biztonsági eseményről a jogszabályban meghatározottak szerint **tájékoztatni** köteles a jogszabályban meghatározott szervet,
- biztosítja a Törvényben meghatározottak követelmények teljesítését a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők tevékenysége esetén.

#### **Rendszergazda feladata:**

- meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai **eszközöket,**
- feladatkörébe tartozó rendszereket **felügyeli, üzemelteti,**
- megszervezi az adatok biztonsági **másolatának** készítését és **karbantartását,**
- gondoskodik a rendszer kritikus részeinek **újra indíthatóságáról,** illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- az adatgazdával együttműködve kialakítja és működteti a **hozzáférési jogosultságok** rendszerét.
- **nyilvántartja** - a jogszabályban definiált adattartalommal - a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos **vírusvédelemről,** vírusmentesítéséről,

- ellenőrzi a **rendszer adminisztrációt**,

### **Adatgazda**

- a használt információkat és adatokat elemzi kezeli,
- az ASP rendszerben TENANT-ként beállítja a Keretrendszert, Szakrendszereket, és ebben felveszi a felhasználókat, és összerendeli a szerepköröket.
- meghatározza – a rendszergazdával - az adatokhoz / tevékenységekhez a hozzáférést, a szükséges-elégéses hozzáférési elv alapján (mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges),
- ASP tanúsítványok kiadása – rendszergazdával – az önkormányzati felhasználók között.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rögzített felhasználói fiókokat és az eSZIG összerendeléseket elvégzi,
- 
- IBSZ melléklete alapján biztonsági osztályba sorolja az általa kezelt adatokat, illetve elektronikus információs rendszert,
- meghatározza – a rendszergazdával - az adatokhoz / tevékenységekhez a hozzáférést, a szükséges-elégéses hozzáférési elv alapján (mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges),
- engedélyezi vagy megtiltja a hozzáféréseket a hatáskörébe tartozó adatokhoz, elektronikus információs rendszerekhez.

### **Felhasználó**

- A felhasználó **jogosult** a munkájához szükséges eszközök használatára, szoftverek, adatok jogosultsági szintje szerinti elérésére. A munkavégzéshez szükséges informatikai, szakmai képzettséget köteles megfelelő szinten tartani.
- A felhasználó **felelős** a szabályok betartásáért, az információk bizalmasságának megfelelő kezeléséért, valamint a személyes használatba vett eszközök védelméért. A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos más felhasználó jogosultságainak használata, ide értve az ASP rendszerben más eSZIG – jének használatával belépni, illetve autentikáció céljából saját eSZIGjét – átadni.
- A Hivatali alkalmazottak csak a Hivatal tulajdonát képező számítógépeket és engedélyezett szoftvereket használhatják. Ettől eltérni csak engedéllyel lehet. A Hivatal számítógépeire szoftvereket telepíteni, és azokat futtatni tilos. Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett. **Köteles** azonnal értesíteni felettesét minden olyan körülményről, amely az informatikához kapcsolódó tevékenység fennakadásához, megszűnéséhez vezethet.

#### **II.1.3.4. Viselkedési szabályok az interneten**

##### **Tilos:**

- A Hivatal kapcsolatos információk nyilvános internetes oldalon való illegális közzététele,
  - Google Drive, One Drive, stb.
- Chat, fájlcsere, nem szakmai letöltés, tiltott oldalak megnyitása, közösségi oldalak használata, magánpostafiók elérés és más, a szervezettől idegen tevékenységet folytatni.

#### **II.1.4.Rendszer és szolgáltatás beszerzés**

##### **II.1.4.1. Beszerzési eljárásrend**

A Jegyző a Hivatal költségvetési határozatába beépíti a beszerzés forrásait. Az eljárásrendet a beszerzési szabályzat tartalmazza, mely az elektronikus információs rendszer, és az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg. Az eljárásrendben meg kell határozni a biztonsági intézkedések követelményeit, melyeket a szerződésben szerződéses követelményként fel kell sorolni a későbbi számon kérhetőség érdekében.

A biztonsági követelmények megfogalmazása *az igények megismerése után* az IBF feladata.

##### **II.1.4.2. A rendszer fejlesztési életciklusa**

A Hivatal saját fejlesztésű szoftvert nem alkalmaz. A beszerzések alkalmával kötött szerződések szabályozzák az adott szoftver rendszerkövetési elvárásait, az elektronikus információs rendszer teljes életútjára vonatkozóan.

A rendszer életciklus szakaszai: követelmény meghatározás, beszerzés, értékelés, üzemeltetés és fenntartás, kivonás (archiválás, megsemmisítés).

##### **II.1.4.3. Külső elektronikus információs rendszerek szolgáltatásai**

A Hivatal a szolgáltatási szerződésben követelményként fogalmazza meg az általa igénybe vett elektronikus információs rendszerekkel szembeni elvárásokat, hogy ezek megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek. *Dokumentálja a külső szervezet feladatait és a kezelt adatok és folyamatokkal kapcsolatos kockázatok szerint a információbiztonsági követelményeknek való megfelelést ellenőrzi.*

### **II.1.5. Emberi tényezőket figyelembevevő – személyi- biztonság.**

Az elvárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet.

A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket, valamint tájékoztatást kell nyújtani arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége vonatkozik az esetleges otthon végzett munkára, illetve a munkaidőn túli munkavégzésre is.

Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Hivatal munkatársa, az elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötése során kell, mint kötelezettséget érvényesíteni.

#### **II.1.5.1. Eljárás a jogviszony megszűnésekor**

A Jegyző a Hivatal dolgozóinak foglalkoztatására vonatkozó jogi szabályozásnak megfelelően a munkaviszony *megszűnését megelőzően* megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez, *visszaveszi a szervezet tulajdonát képező információbiztonsággal kapcsolatos eszközöket. Teljességgel kizárja, hogy a dolgozó visszavont hozzáféréssel elérhető információkhoz továbbra is hozzáférjen.* Megszünteti a személy egyéni hitelesítő eszközeit, és tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről. *A megszűnéskor arra törekszik, hogy a dolgozó által az elektronikus információs rendszer biztonságát vagy jogszabályt sértő magatartás ne következhesen be.*

A jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket, *különös tekintettel a rendszer üzemeltetését végzőkre.*

#### **II.1.5.2. Fegyelmi intézkedések**

A Hivatal belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben.

Amennyiben az elektronikus információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.



## **II.1.6. Tudatosság és képzés**

### **II.1.6.1. Képzési eljárásrend**

A Jegyző megfogalmazza, és kihirdeti a képzési eljárásrendet. A képzési eljárásrendben ki kell térni arra, hogy az elektronikus információs rendszereket csak olyan személyek használhatják, akik megfelelő számítástechnikai, informatikai, valamint szakmai ismeretekkel rendelkeznek az adott szoftver alkalmazásához.

Magasabb informatikai szaktudást igénylő munkakörök betöltése esetén a szükséges szakirányú képzésben kell résztvenni.

A képzési eljárásrendeletben *hivatal legalább a jogszabály által meghatározott gyakorisággal történő oktatással* gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. *A hivatal dolgozóinak a választható kötelező továbbképzések során javasolt informatikával, információbiztonsággal vagy adatvédelemmel kapcsolatos képzésekben részt venni.*

Az SZMSZ-ben ki kell térni az új dolgozó munkába lépésekor az oktatással kapcsolatos teendőkre.

Az oktatáson, illetve továbbképzésen való részvétel az elektronikus információs rendszerrel kapcsolatba kerülő személyek számára kötelező és a megjelenést a résztvevők aláírásukkal kötelesek tanúsítani.

### **II.1.6.2 Biztonság tudatosság képzés**

A Jegyző annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára.

A rendszergazda gondoskodik arról, hogy új elektronikus információs rendszerek bevezetését szoftver bemutató illetve részletes rendszer használat, tesztelés, dokumentáció megismerés előzze meg az érintett dolgozók tekintetében.

A jelenleg használatban lévő elektronikus információs rendszerek cseréje esetében a rendszergazda és az adatgazda fokozott figyelemmel jár el az adatok megőrzése, védelme tekintetében és ezt tudatosítani kell.

Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

### **II.1.6.3. Belső fenyegetés**

A biztonság tudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.

Ha a számítástechnikai rendszer üzemeltetése során kiderül a biztonság megsértése, illetve megsérülése, haladéktalanul meg kell kezdeni a vonatkozó intézkedések érvényesítését. Az eseményt észlelő dolgozónak dokumentálni kell (Informatikai eseménynapló) a megtörténteket, és tájékoztatni kell a közvetlen felettest valamint a rendszergazdát.

Az informatikai rendszert ért káresemények utólagos elemzését szükség esetén el kell végezni. (pl.: hardver hibák, szoftver hibák, bejelentkezések, hozzáférési kísérletek, gondatlan kezelések, vírusok stb.). Az IBF-nek kivizsgálást kell kezdeményeznie a beérkezett jelentés alapján és javaslatot kell tennie a jegyző részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

## **II.2. Fizikai védelmi intézkedések**

### **II.2.1. Fizikai és környezeti védelem**

Meg kell határozni a tűz-, és személyvédelmi, valamint a Hivatal tevékenységéből adódó – bárki által szabadon látogatható – ügyfélszolgálati területekre vonatkozó szabályokat.

#### **II.2.1.1. Fizikai védelmi eljárásrend**

A Hivatal helyiségeiben ügyfélfogadási időpontokban, megfordulhat nem Hivatali dolgozó, ezért különös figyelmet kell fordítani arra, hogy ezekben az irodákban ügyfél nem tartózkodhat egyedül. A számítógépet, más irodatechnikai gépet az ügyintéző távollétében kikapcsolt állapotban kell tartani.

Az irodában elhelyezett számítógép, monitor elhelyezését lehetőség szerint úgy kell kialakítani, hogy a monitor képernyőjén lévő adatokra az ügyfélnek ne legyen rálátása. Az irodákban lévő dokumentumokhoz, iratokhoz az idegenek hozzáférését meg kell akadályozni. A fontosabb számítástechnikai eszközöket, dokumentumokat tartalmazó helyiségeket biztonsági zárral zárni kell, a kulcskezelést szabályozottan kell végezni. *A fizikai védelmi eljárásrendet szükség esetén felül kell vizsgálni.*

**Tűzvédelmi szabályokat a számítástechnikai eszközök esetében minden esetben fokozottan be kell tartani.**

**Tűzvédelmi szempontból a számítástechnikai eszközöket tartalmazó helyiségekben atűz- és munkavédelmi rendszabályokat be kell tartani és tartatni.** A Hivatal helyiségei a „D” tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. A

Hivatal helységeiben a tűzvédelmi szabályzatban meghatározott számú tűzoltó készüléket kell elhelyezni, *a mindenkor hatályban lévő tűzvédelmi előírásokat betartani.*

Gondoskodni kell a megfelelő számú adatmentésről amelyet tűzbiztos páncélszekrényben kell őrizni.

A **feszültség - kimaradás**, ingadozás okozta károk elkerülése szempontjából a fontosabb számíttástechnikai erőforrásokat (pl. szerverek) szünetmentes tápegységgel kell ellátni.

#### **Illetéktelen behatolás**

A Hivatal épületeit biztosítani kell, és a biztosítási feltételeknek megfelelő riasztó és védelmi eszközökkel kell ellátni.

#### **II.2.1.2. Fizikai belépési engedélyek**

Azokra az irodákra vonatkozóan, ahol ügyfelezést a Hivatal nem folytat, össze kell állítani azon személyek listáját, akik jogosultak a területekre történő belépésre.

A listát a Jegyző hagyja jóvá.

#### **II.2.1.3. A fizikai belépés ellenőrzése**

A Hivatal épületeiben be-, és kiléptető rendszer nincs. Az épületbe történő belépés a be-, és kilépési pontokon biztosított. Kísérettel kell ellátni a létesítménybe ad-hoc belépésre jogosultakat és figyelni a tevékenységüket, *a belépési pontokon az egyéni belépési engedélyeket ellenőrzi.* A Jegyző felhívja a Hivatal dolgozóinak figyelmét a rendellenességek jelentésére. *A jegyző összeállítja, és szükség esetén módosítja az információs rendszerekhez hozzáférésre jogosultak listáját, ezekre a területekre csak a listában szereplők és a jogszabály által meghatározott szerepkörben fellépő személyek léphetnek be az engedélyük céljának megfelelő célból.*

### **II.3. Logikai védelmi intézkedések**

#### **II. 3.1. Konfiguráció kezelési eljárásrend**

A Hivatal megfogalmazza, és az érvényes követelmények szerint dokumentálja, majd kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

##### **II. 3.1.1. Konfiguráció kezelés**

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központilag tárol információkat így segíti a felügyeletet, problémakezelést, változáskezelést és a kiadáskezelést. A fentiek figyelembevételével a Jegyző gondoskodik az informatikai eszközökről készült leltár folyamatos karbantartásáról, valamint a szerviz szolgáltatások nyilvántartásáról. A

rendszergazda feladata, amennyiben az alapkonfigurációtól eltérő konfiguráció szükséges vagy nincs alapkonfiguráció, hogy a konfiguráció reprodukálásához szükséges mértékben erről feljegyzést készítsen vagy ha lehetséges, akkor a konfigurációs beállításokat elmentse. A konfigurációs beállításoknál figyelembe kell venni, hogy a jogosultságok a szükséges minimum elv alapján legyenek kiosztva úgy, hogy a funkcionalitás még ne sérüljön. A konfigurációs beállításokat a rendszeres karbantartás során ellenőrizni kell.

#### **II.3.1.2. Alapkonfiguráció**

A Hivatal az informatikai eszközeiről készített leltárban a beszerzési állapotnak megfelelő, alapkonfigurációt tartja nyilván, amely kiindulási alapként szolgál a továbbfejlesztéseknél. Az elfogadott alapkonfigurációk és az azokhoz képest végrehajtott jóváhagyott változtatások révén jönnek létre a jóváhagyott aktuális konfigurációk.

#### **II.3.1.3 Elektronikus rendszerelem leltár**

A Hivatal leltárt készít az elektronikus információs rendszer elemeiről, előírt adattartalommal. Meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt, gondoskodik arról, hogy a leltár pontosan tükrözze az elektronikus információs rendszer aktuális állapotát, az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza.

#### **II.3.1.4. A szoftverhasználat korlátozásai**

A Hivatal kizárólag olyan szoftvert és hozzátartozó dokumentációt lehet használni, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak. A jegyző által engedélyezett, megfelelő licence-el rendelkező szoftvereket lehet használni, melyekről leltár készül.

Szabad vagy nyílt forráskódú vagy *ingyenes* szoftverek használatbavételét a Jegyző engedélyezi. A szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell.

A másolatok és szétosztások ellenőrzése érdekében a telepítőkészleteket *biztonságosan* kell tárolni és a hozzáféréseket ellenőrizni kell.

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

#### **II.3.1.5. A felhasználó által telepített szoftverek**

A felhasználók semmilyen alkalmazást nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a kiszolgálókra és munkaállomásokra csak a rendszergazda végezheti el. Ezen szabályok ellenőrzését a rendszeres karbantartás során a rendszergazda ellenőrzi és az ezen szabállyal ellenétesen

telepített szoftvereket törli, az esetet a jegyzőnek ill. a IBF-nek jelenti, az ilyen módon fellelt szoftverek telepítésének körülményeit lehetőség szerint megvizsgálja.

### **II.3.2. Ügymenet folytonosság tervezése**

#### **II.3.2.1. Ügymenet folytonosságra vonatkozó eljárásrend**

A Hivatal a folyamatos ügymenet biztosítása érdekében tervet készít az elektronikus rendszerek kiesése esetében az elvégzendő feladatokra. A folytonosság védelme érdekében a munkaköri leírásokban, *belső szabályozásban* illetve megbízási szerződésekben rögzíti a katasztrófa okozta helyzetek kezelését, és helyreállítási teendőit.

#### **II.3.2.2. Ügymenet folytonossági terv informatikai erőforrás kiesésekre**

A Hivatal az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével. Meghatározza az alapeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket.

Rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről. Megnevezi a vészhelyzeti szerepköröket, felelőségeket, a kapcsolattartó személyeket. Fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

Kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

#### **II.3.2.3. Az elektronikus információs rendszer mentései**

A Hivatal a saját gépein lévő, az elektronikus információs rendszerben tárolt felhasználószintű információkról, mentést végez az összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Az adott alkalmazások adatainak mentési ciklusait aszerint kell meghatározni, hogy az esetleges adatvesztés pótlása egy embernappal helyreállítható legyen. A folyamatos munkavégzések esetében naponta célszerű az adatok mentését megoldani, amelyet az adatgazda, a rendszergazda, a felhasználó végezhet, ill. szükség esetén *automatikus mentés fut le. Amennyiben automatikus mentés használnak az elkészült mentés használhatóságát ellenőrizni kell.*

Azoknál az alkalmazásoknál ahol a feldolgozások gyakorisága nem napi szintű, az adatmentést elégséges a munkavégzések gyakoriságának megfelelően elkészíteni.

Kétszintű adatmentést kell készíteni, az esetleges katasztrófa helyzetek okozta károk elkerülése érdekében. Az adatmentéseket, valamint a szoftverek telepítő, installáló lemezeit az arra kijelölt, megfelelő biztonsággal ellátott helyiségben, berendezésben kell tárolni. Az adatok mentése és a szoftverek telepítése, újra installálása a rendszergazda feladata. Visszaállítást is végezheti a rendszergazda, de szükség esetén a fejlesztő segítségét kell igénybe venni, aminek feltételeit a rendszerkövetési vagy egyéb megállapodásban rögzíteni kell. Az archiválási kötelezettségeket az ASP szolgáltatást használó rendszerek esetében a Magyar Államkincstár végzi a 466/2017. (XII. 28.) Korm. rendelet alapján.

### **II.3.3. Karbantartás**

#### **II.3.3.1. Rendszer karbantartási eljárásrend**

A Hivatal a karbantartásokat ütemezetten, a javításokat igény szerint hajtja végre. A szerviz, valamint az ASP szolgáltatóval kötött szerződésekben rögzíteni kell a karbantartási feladatokat és a karbantartások gyakoriságát.

Az üzemeltetési tevékenység során a rendszergazda rendszeresen teszteli a beépített információbiztonsági intézkedések megfelelőségét és hatékonyságát.

#### **II.3.3.2. Rendszeres karbantartás**

A rendszergazda feladata:

- a karbantartásokról és javításokról a nyilvántartás vezetése,
- jóváhagyni és ellenőrizni a karbantartási tevékenységet,
- az elszállításra kerülő gépen tárolt adatok, információk mentése.
- ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági és *funkcionális* ellenőrzésnek veti alá azokat.

A Hivatal berendezéseit csak szállító levél kiállításával, valamint a Jegyző engedélyével lehet elszállítani. Az elszállított gépekről törölni csak azokat az adatokat kell amelyek adatvédelem szempontjából védett adatnak minősülnek.

### **II.3.4. Adathordozók védelme**

#### **II.3.4.1. Adathordozók védelmére vonatkozó eljárásrend**

Az adathordozók védelmére vonatkozó eljárásrend magába foglalja a számítógépek, adathordozók biztonságos, megbízható működtetésének feltételeit, miszerint:

- vagyonvédelmi, valamint működés biztonsági szempontból figyelembe kell venni a fentiekben a szervizelésre, karbantartásra vonatkozó meghatározásokat,
- az adathordozókhoz való hozzáférést, ezek használatát, az adatok törlési jogát szabályozza.

- Az adathordozók kezelésénél a tartalmazott adatok szellemébenfigyelembe kell venni az egyenértékű papír dokumentumok kezelésével kapcsolatos előírásokat.

Az adathordozók védelmére vonatkozó eljárásrend más belső szabályozásában (SZMSZ, Munkaköri leírások) is meghatározásra kerül.

Az számítógépek belső adathordozóihoz a rendszergazda férhet hozzá. Szükség esetén külső adathordozókhoz az adatgazda és a jegyző engedélyével férhetnek hozzá vagy használhatják, figyelembe véve a rendszerbiztonsági és adatvédelmi szabályokat.

#### **II.3.4.3. Adathordozók törlése**

A helyreállíthatatlanságot biztosító törlési technikákkal *vagy az adathordozó teljes fizikai megsemmisítésével* törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy *(törlés esetén)* újrafelhasználásra való kibocsátás előtt. *Az adatok vagy adathordozó megsemmisítéséről a megsemmisítést végző feljegyzést készít.*

#### **II.3.4.3. Adathordozók használata**

A Hivatal csak engedélyezett adathordozót szabad használni. A szervezet vezetője, a rendszergazda, illetve *az* adatgazda a hozzáférési jogosultságok szabályozásával *engedélyezheti*, korlátozza, vagy *tilthatja* egyes, vagy bármely adathordozó típusok, és az elektronikus információs rendszerek használatát.

Hordozható adathordozókat a jegyző kivételes engedélyével lehet gépre csatlakoztatni az adathordozó elkülönített módon való vizsgálata után. Adatot tartalmazó adathordozót csak a jegyző engedélyével lehet a szervet telephelyéről kivinni, meghatározott célból és ideig.

#### **II.3.5. Azonosítás és hitelesítés**

##### **II.3.5.1. Azonosítási és hitelesítési eljárásrend**

A Hivatal valamennyi számítógépére a bejelentkezést azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz, és milyen tevékenységet végezhet. Törekedni kell olyan alkalmazások használatára, amelyek többszintű hozzáférési jogosultságra adnak lehetőséget. A jogosultsági szintek kiosztását a dokumentálni kell.

##### **II.3.5.2. Azonosítás és hitelesítés**

A Hivatalban törekedni kell olyan elektronikus információs rendszer, alkalmazás, használatára, ami képes egyedileg azonosítani a felhasználót, és a felhasználó által végzett tevékenységet. Meg kell határozni, a hozzáférési jogosultságok alapján, az egyedi hozzáférést biztosító azonosítókat.

#### **II.3.5.3. Azonosító kezelés**

Az rendszergazda hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz, meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását, meghatározott időtartamú inaktivitás esetén letiltja az azonosítót. Az ASP rendszerben ez az adatgazda feladata. (Tenant)

#### **II.3.5.4. A hitelesítésre szolgáló eszközök kezelése**

A rendszergazda, *amennyiben ilyen eszköz használatban van*, ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát, meghatározza annak kezdeti tartalmát. *Meghatározza a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, meghatározza a minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit. Lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor. A hitelesítésre szolgáló eszköz használója köteles megőrizni rendelkezésére bocsátott eszköz bizalmasságát és sértetlenségét. A hitelesítésre szolgáló eszközt másnak átadni szigorúan tilos! Amennyiben ez a szabály sérült, ennek tényét jelzi a szervezet vezetője felé, aki intézkedik a kapcsolódó jogosultságok visszavonásáról, szükség szerint az eszköz cseréjéről. Hitelesítésre szolgáló eszköz használatbavételekor, amennyiben van alapértelmezett értéke, ezt meg kell változtatni, e-nélkül nem vehető használatba!*

#### **II.3.5.5. A hitelesítésre szolgáló eszköz visszacsatolása**

Az elektronikus információs rendszer fedett visszacsatolást (nem szolgáltat hibás bejelentkezés esetén használható információt) biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

#### **II.3.5.6. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)**

Az elektronikus információs rendszerhez a hozzáférési jogosultságot a rendszergazda biztosítja az engedélyezett feladatok és tevékenységek alapján *a jegyző vagy az általa felhatalmazott személy engedélyével, az általa engedélyezett és szükséges időtartamra. A felhasználót az ilyen módon kiadott jogosultság egyedileg kell, hogy azonosítsa.*

#### **II.3.5.7. Hitelesítés szolgáltatók tanúsítványának elfogadása**

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által



kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

### **II.3.6. Hozzáférés ellenőrzése**

#### **II.3.6.1. Hozzáférés ellenőrzési eljárásrend**

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt *és/vagy* bárki által megismerhető adatok,
- bizalmas *és belső szabályozóval védett* adatok
- személyes 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. Az érintettekkel ezt 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 is biztosítani kell (szoftver, hardver adatvédelem).

A szervezet az információs rendszerében nem kezel minősített adatot, kiemelt védelemben részesített különleges személyi adatot.

A rendszergazda hozzáférés védelmére vonatkozó eljárásrendben meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférések védelmére vonatkozó eljárásrendet.

#### **II.3.6.2. Felhasználói fiókok kezelése**

A rendszergazda meghatározza:

- és **azonosítja** az elektronikus információs rendszer felhasználói fiókjait, és ezek típusait,
- **megnevezi** az elektronikus információs rendszer jogosult felhasználóit, és a hozzáférési jogosultságokat,
- **kijelöli** a felhasználói fiókok fiókkezelőit,
- **ellenőrzi** a felhasználói fiókok használatát, és szükség esetén törli ezeket.

*Külső közreműködők által üzemeltetett rendszerek esetén (pl. weboldal, ASP szolgáltatás) a fentieket azzal az eltéréssel kell alkalmazni, hogy ha a rendszergazda közvetlenül nem tudja a fiókokat kezelni, értesíti az üzemeltetőt vagy egyéb fiókkezelőt a fiókok létrehozásának vagy megszüntetésének vagy módosításának szükségességéről.*

### **II.3.6.3. Hozzáférés ellenőrzés érvényesítése**

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez. A hivatal vezetője határozza meg, hogy a felhasználó hogyan és milyen adatkörben jogosult külső információs rendszerben a hivatal által ellenőrzött adatokat feldolgozni.

### **II.3.6.4. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek**

A Hivatalnál nincs azonosítás vagy hitelesítés nélkül engedélyezett tevékenység.

### **II.3.6.5. Külső elektronikus információs rendszerek használata**

Az elektronikus információs rendszer felügyelete. A Hivatal tevékenységéből adódóan nem indokolt külső rendszerből hozzáférni a hivatalban működő elektronikus informatikai rendszerhez. Amennyiben erre mégis szükség van, az IBF-fel és a rendszergazdával egyetértésben, meghatározott célból, meghatározott ideig engedélyezhető a külső hozzáférés úgy, hogy a hozzáférést végző személye azonosítható legyen.

### **II.3.6.6. Nyilvánosan elérhető tartalom**

A Hivatal honlapjai nyilvánosan hozzáférhető információkat tartalmaz. A honlap kezelésére kijelölt személy felelős azért, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat, valamint az adattartalom valós, hiteles legyen. A szervezet vezetője vagy az általa felhatalmazott személy a felelős személyt kioktatja annak biztosítása és felismerése érdekében, hogy a nyilvánosan elérhető információk ne tartalmazzanak nem nyilvános információkat. A szervezeten belül egy az adatokkal kapcsolatosan kompetens személynek át kell vizsgálnia a javasolt tartalmat közzététel előtt. A közzétett tartalmakat rendszeresen át kell vizsgálni annak érdekében, hogy ne tartalmazzanak nem nyilvános információt és/vagy elavult, téves információkat.

## **II.3.7. Rendszer és információsértetlenség**

### **II.3.7.1. Kártékony kódok elleni védelem**

Az elektronikus információs rendszert annak belépési és kilépési pontjain védeni kell a kártékony kódok ellen. A Hivatal számítógépeire, illetve szerverre víruskereső szoftvert kell telepíteni. A szoftver rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a

végpontokon. A kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és jelezzen a felhasználónak. A felhasználó értesítse a rendszergazdát, aki elvégzi az ügymenet folytonosságra vonatkozó követelmények figyelembevételével a szükséges intézkedéseket a kártékony kód megsemmisítése és az esetleges kár felmérése érdekében.

#### **II.3.7.2. Az elektronikus információs rendszer felügyelete**

A rendszergazda feladata az elektronikus információs rendszer felügyelete a következők szerint:

- azonosítja az elektronikus információs rendszer jogosulatlan használatát,
- védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
- meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

#### **II.3.7.3. A kimeneti információ kezelése és megőrzése**

A Hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

### **II.3.8. Naplózás és elszámolhatóság**

#### **II.3.8.1. Naplózási eljárásrend**

A szolgáltató felelőssége, hogy a Hivatalnál olyan alkalmazás működjön, amely a rendszerhez való hozzáférést, az adatokkal kapcsolatos tevékenységeket naplózza, annak érdekében, hogy ezáltal ezek a tevékenységek később visszakereshetők legyenek. A rendszergazda a naplófájlokat rendszeresen megnézi, s a jogosulatlan hozzáférést vagy annak a kísérletét jelenti a Jegyzőnek.

#### **II.3.8.2. Naplózható események**

Az adatgazda meghatározza naplózandó eseményeket, és megvizsgálja, hogy az alkalmazások naplózható eseményei megfelelőek-e, a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

#### **II.3.8.3. Naplóbejegyzések tartalma**

Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

- felhasználó megnevezése
- végzett tevékenység
- időponthoz rendelés

#### **II.3.8.4. Időbélyegek, rendszeridő**

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek (A Hivatalon belül szinkronizált) előállításához, amely rögzíti a naplóbejegyzések időpontjait. A számítástechnikai eszközök órájának beállítását kizárólag a rendszergazda végezheti. A felhasználó kötelessége jelezni, ha egy rendszeróra nem a megfelelő időt tartalmazza.

#### **II.3.8.5. A naplóinformációk védelme**

A szolgáltatónak biztosítania kell, hogy a naplóállományokhoz illetéktelen személyek ne férhessenek hozzá, ezeket módosítani, megsemmisíteni ne tudja. Az állományok mentésénél figyelembe kell venni azok méretét.

#### **II.3.8.6. A naplóbejegyzések megőrzése**

A naplóadatokat kritikusságuknak megfelelően osztályozni kell, és a jogszabályi előírás szerinti ideig meg kell őrizni. Biztosítani kell az állományok megőrzését a kivizsgálás lezárásáig. Az érintett szervezet a naplóbejegyzéseket egy évig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

#### **II.3.8.7. Naplógenerálás**

Az elektronikus információs rendszereknek *lehetőség szerint* biztosítania kell a naplóbejegyzés generálási lehetőségét a naplózható eseményekre, személyhez kötötten, a fentiek alapján.

### **II.3.9. Rendszer és kommunikációvédelem**

#### **II.3.9.1. Rendszer- és kommunikációvédelmi eljárásrend**

A Hivatal a rendszer- és kommunikációvédelmi eljárást az alábbiaknak megfelelően határozza meg.

#### **II.3.9.2. A határok védelme**

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt.

- a nyilvánosan hozzáférhető rendszerelemeket elkülöníti a belső szervezeti hálózattól,
- csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez,

- A Hivatal hálózatában csak olyan Wi-Fi eszköz csatlakoztatható, amely minimum WPA2 (technikai korlátok esetén WPA) titkosítást alkalmaz. Csak olyan eszköz csatlakoztatható, amely a hivatal használatában és felügyelete alatt áll és megfelel jelen szabályzatnak.
- az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom szűrésére, ellenőrzésére a lehetőségek korlátozására tűzfalakat, tartalomszűrőket, illetve meghatározott címekkel a kapcsolat tiltását biztosító megoldásokat kell alkalmazni.

### **II.3.9.3 Kriptográfiával kapcsolatos szabályozás**

Amennyiben a szervezet kriptográfiai eljárást használ, ez csak szabványos eljárás lehet. A használat módja lehetőség szerint az aktuálisan elfogadott modern algoritmusokat használja, kerülve a régi vagy ismert sebezhetőségekkel rendelkező eljárásokat. A kommunikációs csatornák kriptográfiai védelmére törekedni kell, a lehetőségek szerint a technikailag és a rendelkezésre álló szoftver lehetőségei szerint a használatkor ismert biztonságos konfigurációt használhat, ezt rendszeresen felül kell vizsgálni.

Amennyiben a szervezet maga állít elő vagy használ más által generált kriptográfiai kulcsot, így annak szabályozására, tárolására, megsemmisítésére szabályozást készít a kriptográfiával védett adat milyenségével összhangban.

Kriptográfiai eszköz vagy szoftver alapértelmezett beállításokkal, telepítés során létrejött vagy a telepítőcsomagban található értékekkel (beleértve, de nem kizárólagosan privát kulcs, alapértelmezett titkosítási jelszó, előre beállított DH-paraméter, stb.) nem vehető használatba.

### **II.3.9.4 Együttműködésen alapuló számítástechnikai eszközök**

A szervezet működéséhez alapvetően nincs szükség olyan informatikai eszközre, ami kamerát és/vagy mikrofont használ. Amennyiben a számítógép tartalmaz ilyet, ezt inaktíválni kell. Külső mikrofont vagy kamerát tilos számítógépéhez csatlakoztatni. Amennyiben ilyen szoftver használatára esetleg mégis szükség van, ezt a jegyző az IBF-fel egyetértésben engedélyezheti, de az alkalmazott kamera, mikrofon csak a használat időtartama alatt lehet csatlakoztatva és csak olyan kamerát lehet csatlakoztatni, ami jelzi az aktivitást.

### **II.3.9.5. A folyamatok elkülönítése**

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

**A Balatonkeresztúri Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata**  
**2018. év január hó 01. napjával lép hatályba.**

Balatonkeresztúr, 2017. 12. 28.

Jóváhagyta, kiadta :

  
\_\_\_\_\_  
**Mestyán Valéria**  
**Címzetes Főjegyző**  


### **III. Jogszabályi hivatkozások**

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)

41/2015. (VII. 15.) BM rendelet

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

42/2015. (VII. 15.) BM rendelet

az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

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

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.)

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

1995. évi LXVI. törvény a közokiratokról, a közlevéltárakról, és a magánlevéltári anyag védelméről

1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

2001. évi XXXV. törvény az elektronikus aláírásról

1993/146. (X. 26.) Korm. rendelet a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról

MSZ ISO/IEC 27001:2006: Az információbiztonság irányítási rendszerei. Követelmények

A KIB 25. számú ajánlása: Magyar Információbiztonsági Ajánlások (MIBA) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások

A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár

valamint az ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet figyelembe vételével, illetve a 466/2017. (XII.28.) Korm. rendelet az elektronikus ügyintézésrel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezzorról – készült.

#### **IV.Értelmező rendelkezések**

**adat:** az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

**adatfeldolgozás:** az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

**adatfeldolgozó:** az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;

**adatkezelés:** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

**adatkezelő:** az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;

**adminisztratív védelem:** a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

**auditálás:** előírások teljesítésére vonatkozó megfeleléségi vizsgálat, ellenőrzés;

**ASP:** Alkalmazás-szolgáltatás, vagy alkalmazás-bérlet, amely egy új üzleti és egyben technológiai konstrukciót jelent.

Az ASP keretében a felhasználók a tevékenységük támogatásához szükséges ügyviteli, vagy egyéb szoftvereket úgy veszik igénybe, hogy interneten keresztül kapcsolódnak a szolgáltatónál elhelyezett szerverekhez, az ezeken működő adatbázisokhoz és az adatokat kezelő programokhoz. A felhasználói gépeken csak egy egyszerű böngészőprogramnak kell futnia és internet kapcsolattal kell rendelkeznie.

**bizalmasság:** az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

**biztonsági esemény:** nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

**biztonsági esemény kezelése:** az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés



okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

**biztonsági osztály:** az elektronikus információs rendszer védelmének elvárt erőssége;

**biztonsági osztályba sorolás:** a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

**biztonsági szint:** a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

**biztonsági szintbe sorolás:** a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

**elektronikus információs rendszer biztonsága:** az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

**észlelés:** a biztonsági esemény bekövetkezésének felismerése;

**felhasználó:** egy adott elektronikus információs rendszert igénybe vevők köre;

**fenyegetés:** olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

**fizikai védelem:** a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

**folytonos védelem:** az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

**globális kibertér:** a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

**informatikai biztonságpolitika:** a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

**informatikai biztonsági stratégia:** az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

**információ:** bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

**kiberbiztonság:** a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibertér megbízható környezeté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

**kibervédelem:** a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

**kockázat:** a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

**kockázatelemzés:** az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

**kockázatkezelés:** az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló

intézkedésrendszer kidolgozása;

**kockázatokkal arányos védelem:** az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

**korai figyelmeztetés:** valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

**létfontosságú információs rendszerelem:** az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

**logikai védelem:** az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

**magyar kibertér:** a globális kibertér elektronikus információs rendszereinek azon része, amelyek

Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

**megelőzés:** a fenyegetés hatása bekövetkezésének elkerülése;

**reagálás:** a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

**rendelkezésre állás:** annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

**sértetlenség:** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

**sérülékenység:** az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

**sérülékenység vizsgálat:** az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

**szervezet:** az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint jogi személyiséggel nem rendelkező gazdasági társaság, egyéni vállalkozó;

**teljes körű védelem:** az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

**üzemeltető:** az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

**védelmi feladatok:** megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

**zárt célú elektronikus információs rendszer:** jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;

**zárt védelem:** az összes számításba vehető fenyegetést figyelembe vevő védelem.

## V. Mellékletek

### 1. számú melléklet – IBSZ hatálya alá tartozó költségvetési szervek

- Balatonkeresztúri Közös Önkormányzati Hivatal
- Balatonberény Község Önkormányzata
- Balatonmárfiafürdő Község Önkormányzata
- Balatonkeresztúr Község Önkormányzata

### 2. számú melléklet – Az információs rendszer biztonsági osztályba sorolása

#### Az adatok minősítése

Az adatok, illetve rajtuk keresztül az azokat kezelő alkalmazások és rendszerelemek információvédelemre vonatkozó biztonsági követelményszintje szempontjából a jogszabályok, szabványok, ajánlások és belső utasítások keretében előírt védelmi követelmények meghatározóak. Ezek alapján a védendő adatoknak alapvetően négy csoportját különíthetjük el:

- ” nyílt, szabályozók által nem védett adat,
- ” érzékeny (védendő), de nem minősített adat,
- ” szolgálati titok, államtitok.

Az érzékeny, de nem minősített adatok körébe tartoznak a jogszabályok által védendő adatok (személyes, illetve különleges adatok, az üzleti titkot, a banktitkot képező adatok, az orvosi, az ügyvédi és egyéb szakmai titkok, stb.) és a Hivatal belső szabályozása alapján védendő adatok. A Hivatal az informatikai rendszereinek az adatok információvédelmére vonatkozó követelményszint szempontjából való osztályozása során az adatoknak az említett négy besorolásából csak a nyílt, illetve az "érzékeny" adatokat osztályozzuk. Az ASP teszt rendszer.

Tervezés:						
Alkalmazás neve	Alkalmazás leírása	Adatgazda	A rendszer biztonsági osztálya			
				B	S	R
ASP- KERET	Önkormányzati ASP keretrendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	4	4	4
ASP- ADÓ	Önkormányzati ASP adórendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	4	4	4
ASP GAZDÁLKODÁS	Önkormányzati ASP gazdálkodási rendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	3	3	3
ASP IRATKEZELŐ	Önkormányzati ASP iratkezelő rendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	3	3	3
ASP- HAGYATÉK	Önkormányzati ASP hagyaték leltár rendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	3	3	3
ASP INGATLAN	Önkormányzati ASP ingatlanvagyon rendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	3	3	3

ASP- IPAR és KERESKEDELEM	Önkormányzati ASP ipar és kereskedelmi rendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	3	3	3
ASP- PORTÁL	Önkormányzati ASP települési portál rendszer	Jegyző	Jelenlegi osztály	2	2	2
			MÁK által elvárt	3	3	2
WINIKTAT	Iktatási rendszer	Jegyző	Jelenlegi osztály	2	2	2
VIZUÁL REGISZTER	Népesség nyilvántartás	Jegyző	Jelenlegi osztály	2	2	2
WINSZOC	Szociális nyilvántartás	Jegyző	Jelenlegi osztály	2	2	2
ELEKTRA-OTP	Banki műveletek	Jegyző	Jelenlegi osztály	2	2	2
EBR-42	Önkormányzati információs rendszer	Jegyző	Jelenlegi osztály	2	2	2
ANYK	Nyomtatványkitöltő	Jegyző	Jelenlegi osztály	2	2	2
KGR	Adatszolgáltató modul	Jegyző	Jelenlegi osztály	2	2	2
PTR	Adatszolgáltató modul	Jegyző	Jelenlegi osztály	2	2	2

A fenti táblázat a Magyar Államkincstár által kiadott tájékoztatót figyelembe véve készült.

Az osztályba sorolás alapján az adatok 2-es szint feletti értéket nem értek el. Az elektronikus információs rendszer biztonsági osztálya 2-es szintű.

A Hivatal által használt alkalmazások adatai védelmi intézkedések kialakítása szerint alapvetően az alábbi kategóriába sorolandók:

1. Az alkalmazás a Hivatal gépén fut, az adatok is helyi gépen található.

Védelmi intézkedéseket a Hivatalnak kell megtennie.

2. ASP szolgáltatás igénybevétele.

Szolgáltatói szerződésben kell rögzíteni a védelemmel kapcsolatos elvárásokat.

3. WEB-es szolgáltatások.

Az adatok hozzáférés szempontjából nyilvánosak, de az adat sértetlensége miatt az adat tartalom rögzítése, módosítása, törlése hozzáférési jogosultságok alapján történik.

4. Intranet hálózatban futó alkalmazások.

A Hivatal a szolgáltató előírásainak megfelelően jár el, a jogosultsági szintek kialakítása érdekében.

5. Adatszolgáltatások, statisztikák.

Az adatok nyilvánosak.

**A biztonsági osztályba sorolás útmutatója:**

Bizalmasság kárérték-táblázata			
Kárérték szint/Kárfajta	Anyagi kár	Társadalmi politikai hatás	Jogszabályi következmény
1. nem értelmezhető	Nyilvános adat		
2. csekély kár	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.	Kínos helyzet a szervezeten belül	Belső szabályozóval védett adat bizalmassága sérül

Sértetlenség kárérték-táblázata		
Az elektronikus információs rendszer vagy az abban tárolt adat pontatlansága esetén a kár mértéke:		
Kárérték szint/Kárfajta	Anyagi kár	Társadalmi politikai hatás
1. jelentéktelen kár	a közvetlen és közvetett anyagi kár nem éri el az érintett szervezet költségvetésének 1%-át.	Nincs bizalomvesztés, a probléma a szervezeten belül marad
2. csekély kár	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át. 1 embernappal állítható helyre	Kínos helyzet a szervezeten belül a probléma az érintett szervezeten belül marad, és azon belül meg is oldható

Rendelkezésre állás kárérték-táblázata		
Az elektronikus információs rendszer vagy az abban tárolt adatok rendelkezésre állásának elvesztése esetén (nem elérhető a rendszer vagy az adat) a kár mértéke:		
1. jelentéktelen kár	a közvetlen és közvetett anyagi kár nem éri el az érintett szervezet költségvetésének 1%-át.	Nincs bizalomvesztés, a probléma a szervezeten belül marad
2. csekély kár	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át. 1 embernappal állítható helyre	Kínos helyzet a szervezeten belül a probléma az érintett szervezeten belül marad, és azon belül meg is oldható

### **3. számú melléklet – A Hivatal biztonsági szintje**

**A Hivatal biztonsági szintje a jelen IBSZ hatályba lépésekor, rendelkezésre álló dokumentumok, szabályzatok alapján: 2, azaz kettes szint a NEIH által kiadott Osztályba sorolási és Védelmi intézkedési űrlap v4.51 alapján.**

#### 4.számú melléklet - Kockázatelemzési és kezelési módszertan

Az egyes vagyonelemek gyenge pontjait és fenyegetettségét KIB 25. számú ajánlása: 25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata (IBIV) 1.0 verzió segédletei alapján a következőképpen állapítja meg:

A kockázat meghatározása során a veszély megvalósulásának valószínűsége és az okozható kár alapján, az adott veszélyt képviselőszerűlékenység kihasználhatósága és ennek hatása alapján történik. A veszélyeztetett információk vagy azok csoportjaira külön-külön meg kell állapítani a kockázatot, a teljesség kialakítása céljából.

A gyakorlatban célszerű kategóriákkal dolgozni, amelyek az adott környezet működéséhez igazodnak.

A hatások kategorizálása a közigazgatás szemszögéből:

- **Alacsony**, várhatóan korlátozott hátrányos hatást gyakorol a közigazgatási szervezet műveleteire, vagy a szervezet eszközeire.

A korlátozott hátrányos hatás azt jelenti, hogy:

A szolgáltatási képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani ugyan elsődleges funkcióit, de a funkciók hatásossága észrevehetően csökken. Az ügyek lefolytatásában fennakadást okoz, de a sikeres lefolytatást és határidők betartását nem veszélyezteti.

A szervezeti eszközök kisebb mértékűkárosulását eredményezi.

Kisebbs mértékűpénzügyi veszteséget okoz.

A jogbiztonságot kisebb mértékben veszélyezteti, a személyes és/vagy közhiteles adatok védelmével kapcsolatban felmerül a lehetőség, hogy a helyzet javítása nélkül az adatok védelme sérülhet.

- **Fokozott**, várhatóan komoly hátrányos hatást gyakorol a közigazgatási szervezet műveleteire, vagy a szervezet eszközeire.

- **Kiemelt**, várhatóan súlyos vagy katasztrofális hatást gyakorol a közigazgatási szervezet műveleteire, vagy a szervezet eszközeire.

A bekövetkezési valószínűsége lehet:

- **Magas** – bármikor előfordulhat. mert pl. gyakori esemény, vagy a támadást bárki végrehajthatja. Ilyen lehet például egy olyan vírustámadás.

- **Közepes** – gyakran előfordulhat, pl. célzott számítógépes betörés a rendszerbe.

- **Alacsony** – az előfordulása a vizsgált rendszer vagy szervezet működési idejéhez képest nem gyakori. Ilyen lehet például tüzeset vagy természeti csapás.



A várható kár és a bekövetkezés valószínűsége alapján a kockázat is kategorizálható:

Hatás/valószínűség	<i>alacsony</i>	<i>közepes</i>	<i>magas</i>
<i>alacsony</i>	mérsékelt	alacsony	alacsony
<i>fokozott</i>	jelentős	mérsékelt	alacsony
<i>kiemelt</i>	kritikus	jelentős	mérsékelt

## VÉDELMI INTÉZKEDÉSEK

A védelmi intézkedések, alábbi csoportosítása, amely segíti a veszélyekhez rendelt intézkedések kidolgozását, azon az alapon, hogy a veszélyt megelőzni, észlelni, vagy javítani kívánjuk:

- **Megakadályozó** (preventív): a megelőzés során olyan tevékenységeket kell végrehajtani, amely lehetetlenné teszi a veszélyes esemény bekövetkeztét (pl. email tartalomszűrés, amellyel megelőzzük vírusok levelezésen keresztüli bejutását).
  - **Észlelő**(detektáló): az észlelés során a már folyamatban lévő támadást, károkozást próbáljuk – lehetőleg minél hamarabb – észlelni, majd ez alapján megszüntetni, mielőtt lényegi károkozásra kerülne sor. Ilyen például a behatolás jelző (IDS) rendszer használata, amely gyanús hálózati forgalom esetén riasztást ad. Az észlelés alapján azután más tevékenységeket is végezhetünk.
  - **Helyreállító** (korrektív): a javító intézkedés a már megtörtént esemény által okozott kárt csökkenti vagy szünteti meg. Javító intézkedés például a rendszer visszaállítása mentésből, de ilyen intézkedés akár az is, ha biztosítással rendelkezünk, amely kár esetén biztosít fedezetet. Ezt a hármas szokás az angol megnevezések alapján PreDeCo-nak (Preventive – megakadályozó, Detective – észleli, Corrective – helyreállító) nevezni.
- Az egyes veszélyforrásokra vonatkozóan megállapíthatóak a védelmi intézkedések, ezek kidolgozása során használhatjuk a CIA (bizalmasság, sértetlenség vagy rendelkezésre állás) elvet, minden veszélyforráshoz hozzárendelve az általa képviselt kockázatot, az azt megvalósító bizalmasság, sértetlenség vagy rendelkezésre állás sérülését és az ezeket megelőző, detektáló vagy javító intézkedéseket.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
ASP rendszer önkormányza- ti, végponti állomásai	Érzékeny adatok ellopása, adatfájlok törlése, ellopása, módosítása.	Hozzáférés védelem beállítása.
	Rosszindulatú program (vírus, trójai faló, stb.) bejuttatása a rendszerbe.	Vírusvédelmi rendszer alkalmazása.
	Vírus, trójai faló, féreg aktiválódása, pl. e-mail csatolmány megnyitásakor.	Vírusvédelmi rendszer alkalmazása.
	Végrehajtható programok, script-ek (Java Applet, JavaScript, VB Script, CGI, stb.) letöltése, pl. az állomás DoS támadásra való felhasználására a felhasználó tudtán kívül.	Böngésző biztonsági beállítása.
	Web és alkalmazásba csomagolt ActiveX objektumok, amelyek a programozó szándékától függően a legkülönbözőbb károkat (gépleállítás, konfiguráció feltérképezés, monitor/billentyűzet elvétel, stb.) okozhatják.	Böngésző biztonsági beállítása.
	Ismeretlen forrásból érkező e-mail-ek és azok csatolmányainak megnyitása.	Vírusvédelmi rendszer alkalmazása, felhasználó oktatása.
	Az Internet böngészőkben meglévő biztonsági „lyukak” megszüntetésére szolgáló javító programok letöltésének elmulasztása. A biztonsági „lyukak” kihasználásával elérhetők a végponti felhasználó érzékeny adatai (jelszó, az állomás konfigurációja, fájl nevek, fájl struktúra, a meglátogatott weblapok címei, stb.).	Legújabb verziók, frissítések telepítése.
	A munkaállomásra letöltött adatlapok (kérdőív, adatszolgáltató formanyomtatvány, stb.) programhibái. A szolgáltatott adatok rejtjelezés nélküli elküldése.	Csak megbízható forrásból származó program használata.
	Vírusvédelmi program frissítésének elmulasztása.	Rendszeres, automatikus frissítés.
	Az igénybevett szolgáltatás letagadása.	Naplózás.
	A munkaállomás ellopása.	Követelményrendszer szerinti fizikai biztonság kialakítása.
	Mobil eszköz ellopása	Az előírt fizikai védelmi eszközök alkalmazása. Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
Internet	A felhasználó login adatainak (felhasználói-azonosító, jelszó) lehallgatása, ezek segítségével a felhasználó megszemélyesítése.	Rejtjelezett adatátviteli csatorna használata.
	Érzékeny adatok lehallgatása.	Rejtjelezett adatátviteli csatorna használata.
	Adatok lehallgatás és továbbítása megváltoztatott tartalommal elleni védelme.	Hozzáférés-vezérlés kialakítása. Rejtjelezett adatátviteli csatorna. Egyszer használatos jelszó.
	E-mail-ek, elektronikus dokumentumok eltérítése.	Hozzáférés-vezérlés kialakítása.
Tűzfal	Tűzfal-biztonságpolitika hiánya vagy hiányos volta.	Tűzfal-biztonságpolitika elkészítése, vagy aktualizálása.
	Ad hoc vagy nem a biztonságpolitikának megfelelő biztonsági beállítás, vagy üzemeltetés.	Biztonsági beállítások rendszeres ellenőrzése, naplózás, riasztás.
	Portok letapogatása.	Tűzfal biztonsági beállítása.
	IP cím megszemélyesítés, a támadó a védett hálózaton működő számítógép (pl. szerver) IP címét megszerezve egy belső munkaállomást „szimulálva” a tűzfalon keresztül fér hozzá a szerveren levő adatállományokhoz.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása.
	Visszaélés, forrás útvonalválasztással. A támadó a védett belső hálózat felépítésének ismeretében a saját gépében meghatározott útvonallal és belső IP címmel belső gépet „játszik el” és fér hozzá az útvonal végén levő belső géphez.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása. Hálózati végpont IP címhez, MAC címhez kötése.
	Szerver típus specifikus biztonsági lyukak az operációs rendszerben. Az aktuális javító- és szerviz csomagok telepítésének elmulasztása.	Operációs rendszerek biztonsági frissítéseinek folyamatos figyelése, végrehajtása.
	A tűzfal távoli, pl. Interneten keresztül történő adminisztrálása.	Tűzfal adminisztrálása csak védett hálózatról, vagy konzolról.
	Vírusvédelmi programok frissítésének elmulasztása.	Vírusvédelmi rendszer folyamatos frissítése.
	Hiányos biztonsági naplózás. A biztonsági naplók értékelésének elmulasztása vagy rendszertelensége.	Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.

**5. számú melléklet, - Hozzáférés jogosultság igénylő lap**

iktatószám:.....

Jogosultság igénylő neve:	
Szervezeti egység megnevezése:	

Alkalmazás neve:	
Hozzáférési jog:	
Felhasználó azonosító:	
Aktiválást(adatgazda) végző személy:	
Engedélyező vezető:	
Jogosultság kezdete:	
Jogosultság vége:	

**A felhasználó tudomásul veszi, hogy:**

- a rábízott adatokért és jogosultságokért személyes felelősséget vállal,
- felhasználói-azonosítóját és jelszavát nem szolgáltathatja ki más személynek,
- a saját számítógépén és a hozzákapcsolódó rendszerekben létrehozott és kezelt állományok – beleértve az elektronikus levelezést is –, a Pusztakovácsi Község Önkormányzata tulajdonát képezik, ezért a Pusztakovácsi Község Önkormányzata szabályzatokban és utasításokban feljogosított ellenőrző szerveinek, ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van.

.....  
Felhasználó aláírása

.....  
Szervezeti egység vezetője

A jogosultság beállítását végzőszemély olvasható aláírása:

.....

**5. számú melléklet, - Hozzáférés jogosultság igénylő lapok összesítése**

<b>Iktatószám</b>	<b>Alkalmazás neve</b>	<b>Hozzáférési jog</b>	<b>Felhasználó neve</b>	<b>Munkahelyi vezető</b>

**6. számú melléklet, - Biztonsági események jelentése**

iktatószám: \_\_\_\_\_

**A biztonsági esemény megnevezése:**

Észlelés helye:

Az esemény leírása:

201...,.....hó,.....nap.

\_\_\_\_\_  
**Észlelő**

\_\_\_\_\_  
**Címzetes Főjegyző**

**Az esemény kivizsgálásának leírása:**

A tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

201...,.....hó,.....nap.

A Nemzeti Információbiztonsági Hatóság felé a jelentés megtörtént:


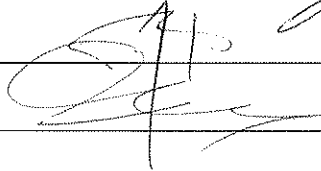
\_\_\_\_\_  
**IBF**

\_\_\_\_\_  
**Címzetes Főjegyző**

7. számú melléklet,

MEGISMERÉSI NYILATKOZAT

Balatonkeresztúri Közös Önkormányzat Informatikai Szabályzatában foglaltakat megismertem, és azt munkám során kötelezően betartom:

NÉV	FELADAT	ALÁÍRÁS
HORVÁTH TIBOR		
TARKANÉ KÖSELMÓNIKA		Tarkané Köselemónika
KIRÁLYNÉ SZABÓ GYÖRGYI		Királyné Szabó Györgyi
MORVÁTH TIBORNÉ		Morvath Tiborné
SZABÓ GÁBOR IMRE		Sabó Imre
SCHENKÉ GÁBRIELLA		Schenke Gabriella
BZOUÁNNÉ KIRÁLY GYÖRGYI		Bzouánné Király Györgyi
KENYELMÓTI KÁSZLONÉ		Kenyelmóti Kászlóné
GÖRZÖNÉ LÁZÁR EDINA		Görzöné Lázár Edina
GÁZDASZKAI KATALIN		Gázdaskai Katalin
NEIMETH GYÖRGYI		Neimeth Györgyi
JANKOVICS GÁBORNÉ		Jankovics Gaborné
BEÖRE AGOTA		Beöre Agota
FEJÉR LÁSZLÓ		
BARVA ELMÉNÉ		



**8. számú melléklet,**

A KÖH weboldalának neve: **www.balatonkeresztur.hu**

A rendszer felett felügyeletet gyakorló neve, és elérhetősége:

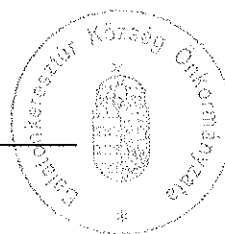
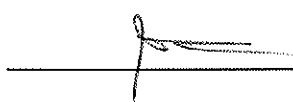
Fentős Károly 70/335-8018

A fejlesztést és karbantartást végzi:

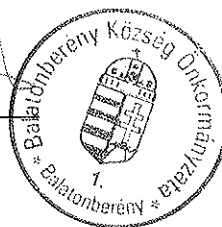
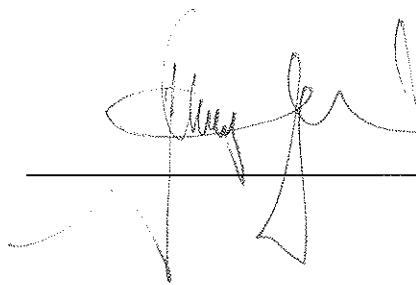
**9. számú melléklet,**

Alulírottak, a Balatonkeresztúri Közös Hivatal fenntartó önkormányzatok polgármesterei a KÖH Informatikai Szabályzatát megismertük, és elfogadtuk.

**Kovács József**  
**Balatonkeresztúr**



**Horváth László**  
**Balatonberény**



**Galács Görgy Vince**  
**Balatonmárfürdő**

