# INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

## Sásdi Közös Önkormányzati Hivatal

Sásd, 2018. 06. 14.

## Tartalomjegyzék

# I. Általános rész

## 1. Az IBSZ célja

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) biztonságkezelési elveket, követelményeket és szabályokat tartalmaz a Sásdi Közös Önkormányzati Hivatal (továbbiakban: a Hivatal) tevékenykedő személyek (bizonyos feltételek esetén külső közreműködők) számára, akik felelősek az információbiztonság fejlesztéséért, megvalósításáért és megtartásáért. Az IBSZ hatékonyan támogatja a Hivatal biztonságkezelésének mindennapi gyakorlatát, illetve megfelelő kereteket biztosít a Hivatal teljes körű biztonsági szabályozásához.

Az IBSZ-ben szereplő követelményeket, rendelkezéseket és ajánlásokat a hatályos jogszabályok keretei között kell használni. A biztonsági szabályozás célja a következő:

a) A jogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit,

b) A tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot,

c) A megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését.

A jelen IBSZ a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. Az IBSZ a hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek és az azokban kezelt adatok biztonságát. Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van.

A Hivatal informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen IBSZ-szel.

## 2. Hatály

### 2.1. Szervezeti-személyi hatály

Az IBSZ szervezeti hatálya a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

Az IBSZ személyi hatálya kiterjed a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), így:

a) a választott tisztségviselőkre (Sásd Város polgármestere, Gödre Község polgármestere),

b) a közszolgálati jogviszony alapján foglalkoztatott munkatársak,

c) a munkaviszony alapján foglalkoztatott munkatársakra,

d) a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre,

e) más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

## 2.2. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed a Hivatal adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes elektronikus információs rendszerre és ezek működési környezetére.

A tárgyi hatály kiterjed továbbá az ezen rendszerek működéséhez alkalmazott szoftverekre, illetve az ezekkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

A tárgyi hatály kiterjed az önkormányzati ASP központ által nyújtott szakrendszerek felhasználó oldali komponenseire, így

a) a munkaállomásokra;

b) a munkaállomásokon futó szoftverekre;

c) kártyaolvasóra;

d) e-Személyire.

## 2.3. Területi hatály

Az IBSZ területi hatálya kiterjed a Hivatal

a) Sásdi székhelyére, valamint

b) a hivatal gödrei kirendeltségére.

## 2.4. Időbeni hatály

Jelen IBSZ a kiadás napján lép hatályba.

# 3. Az IBSZ felülvizsgálata

Az IBSZ eseti módosítására 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 működésében vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

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.

2016. szeptember 3-án hatályba lépett az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet, mely alapján a Hivatalnak 2017. január 1-ével csatlakoznia kell az önkormányzati ASP rendszer önkormányzati adórendszeréhez és a gazdálkodási rendszeréhez, valamint 2017. január 1-ig az ASP valamennyi szakrendszeréhez.

A csatlakozás feltétele, hogy teljesítse a Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.) foglaltakat.

A Hivatal - cselekvési tervében meghatározottaknak megfelelően - időarányosan végzi az Ibtv.-ben foglalt követelményeknek való felkészülést.

A jelen IBSZ az ASP csatlakozási projekt során kapott információk birtokában kerül felülvizsgálatra, valamint az ASP csatlakozási projekt lezárásakor - azaz amikor a Hivatal valamennyi szakrendszerhez csatlakozik - ismét el kell végezni a végleges felülvizsgálatot.

### 3.1. Hatásköri és illetékességi szabályok

Az IBSZ belső használatú dokumentum: a Hivatal elektronikus információs rendszerének felhasználói, illetve egyéb érintettek (a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek, más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetékteleneknek nem adhatják tovább.

## 4. Kapcsolódó dokumentumok

### 4.1. Jogszabályok

a) 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről

b) 2012. évi I. törvény a munka törvénykönyvéről

c) 2012. évi C. törvény a Büntető Törvénykönyvről

d) 2013. évi V. törvény a Polgári Törvénykönyvről

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

f) 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól

g) 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

h) 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

i) 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

j) 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

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

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

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

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

o) 1999. évi LXXVI. törvény a szerzői jogról

p) 2001. évi XXXV. törvény az elektronikus aláírásról

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

r) 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről

## 4.2. Kapcsolódó szabványok, ajánlások

a) MSZ ISO/IEC 27002:2011: Az információbiztonság irányítási gyakorlatának kézikönyve

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

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

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

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

f) Általános szerződési feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI) v1.6

g) Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HSZSZ-ESZIG) v1.3

h) Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz (HR-ESZIG) v1.3

i) Időbélyegzés Szolgáltatási Rend (ISZR) v1.2

j) Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M) v1.6

## 4.3. Az IBSZ-hez kapcsolódó belső dokumentumok

A Hivatal

a) Szervezeti és Működési Szabályzata

b) Iratkezelési Szabályzata

c) Selejtezési Szabályzata

d) Informatikai Biztonságpolitikája

e) Informatikai Biztonsági Stratégiája

f) Cselekvési terve a Sásdi Közös Önkormányzati Hivatalának elektronikus információs rendszereinek elvárt biztonsági osztályainak, illetve a Hivatal elvárt biztonsági szintjének elérésére

# 5. Az IBSZ általános követelményei

Az IBSZ és a jelen IBSZ
*(7. sz. melléklet – Felhasználói Informatikai Biztonsági Házirend)* melléklete (továbbiakban: FIBH előírásainak alkalmazása, betartása), illetve
(2.1 Szervezeti és személyi hatály) betartatása, a pontban megjelöltek számára kötelező.

Az információbiztonsági előírások betartása megvédi a Hivatalt és a *(2.1. Szervezeti-személyi hatály)* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A felhasználók részére a FIBH, a Hivatal vezető tisztségviselői, a rendszergazda, az IBF és az adatgazdák részére a teljes IBSZ előírásai a mérvadók.

**A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. Az IBSZ és a FIBH el nem olvasása nem mentesít a felelősség alól.**

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák a FIBH előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *(8. sz. melléklet – Felhasználói Nyilatkozat)* mellékletében található nyilatkozat aláírása után lehet használatba venni.

# 6. Biztonsági osztályba sorolás

A Hivatalnak az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 7. § (3) bekezdésében meghatározottak figyelembevételével, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló a 41/2015. (VII. 15.) BM rendelet 1. számú melléklete alapján biztonsági osztályba kell sorolnia az elektronikus információs rendszereit, illetve biztonsági szintbe kell sorolnia a szervezetét biztonsági szintbe kell sorolnia.

## 6.1. Biztonsági osztályba sorolás követelménye

A Hivatal elektronikus információs rendszereit a technológiai vhr által előírt módon, külön-külön a bizalmasság, a sértetlenség és a rendelkezésre állás alapfenyegetésségek vonatkozásában egy 5 fokozatú skálán biztonsági osztályba kell sorolni.

A biztonsági osztályba sorolást az elektronikus információs rendszerben kezelt adat bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az elektronikus információs rendszer sértetlenségének és rendelkezésre állásának sérülése esetén bekövetkező kár mértéke alapján kell elvégezni.

Az önkormányzati ASP rendszer szakrendszereit az ASP működtetője sorolja biztonsági osztályba. Az önkormányzat oldali szükséges védelmi intézkedéseket a csatlakozási szerződésben megfogalmazottak szerint kell végrehajtani.

A biztonsági osztályba sorolást mindig kockázatelemzéssel együtt kell végezni.

A biztonsági osztályba sorolást újra el kell végezni, hogy ha

a) jelentős változás következik be Hivatal szervezeti felépítésében;

b) az elektronikus információs rendszerben kezelt adatok bővülnek vagy az adatok köre változik;

c) változnak a hatályos információbiztonságra vonatkozó jogszabályok.

Ha nem történik lényegi változás, a biztonsági osztályba sorolást háromévente felül kell vizsgálni.

A biztonsági osztályba sorolást az IBF készíti elő az adatgazdákkal együttműködve és a jegyző hagyja jóvá.

A felhasználóknak az információ kezelése során tisztában kell lennie az adott információ védelmi igényével és ennek megfelelően kell kezelniük azt.

### 6.2. A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

A Hivatal a technológiai vhr alapján elvégezte az elektronikus információs rendszerek biztonsági osztályba sorolását.

A biztonsági osztályba sorolás eredményét a jelen IBSZ *{2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* melléklete tartalmazza.

## 7. Biztonsági szintbe sorolás

Az Ibtv. 9. §-ának (1) és (2) bekezdései alapján a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet, valamint az elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

### 7.1. A Hivatal biztonsági szintbe sorolása

Az Ibtv. 9. §-ának (4) bekezdése alapján a szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.

A technológiai vhr alapján

**a Hivatal elvárt biztonsági szintje 4-es,**

mivel

a) szakfeladatait támogató elektronikus információs rendszert használ (3-as szint)

b) a következő kritikus adatokat[1] kezel (3-as szint)

c) személyes adatok, adótitok

d) elektronikus információs rendszert üzemeltet (4-es szint).

## 7.2. Szervezeti egységek biztonsági szintbe sorolása

A Hivatal hatályban lévő Szervezeti és Működési Szabályzata alapján a Hivatalban nem működnek az elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységek, ezért azok biztonsági szintbe sorolása nem értelmezhető.

## 7.3. A Hivatal jelenlegi biztonsági szintje

A Hivatal az Ibtv. előírásainak megfelelően megvizsgálta biztonsági szintjét.

A vizsgálat eredménye a *{Cselekvési terv a Sásdi Közös Önkormányzati Hivatalának elektronikus információs rendszereinek elvárt biztonsági osztályainak, illetve a Hivatal elvárt biztonsági szintjének elérésére}* dokumentumban található.

Ennek alapján

**a Hivatal jelenlegi biztonsági szintje: 1**

[1] *Ibtv. 1. §. 32.a kritikus adat: Az info. törvénykönyv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;*

# II. A Hivatal és az elektronikus információs rendszereinek információbiztonsági követelményei

Az *{6. Biztonsági osztályba sorolás}* fejezetben leírtak alapján a Hivatalnak nincsen 2-es biztonsági osztálynál magasabb elektronikus információs rendszere.

Jelen IBSZ az elektronikus információs rendszereire - ahol azt a biztonsági osztályba sorolás indokolja - a 2-es biztonsági osztály követelményeit veszi figyelembe.

A Hivatalnak a jelen IBSZ kiadását követően 90 napon belül cselekvési tervet kell készítenie a következő biztonsági szintre, illetve a 2-es biztonsági osztályra vonatkozó követelmények teljesítése érdekében.

A biztonsági szint és a biztonsági osztályok különbségeire nézve irányadó, hogy addig is törekedni kell az IBSZ-ben foglalt követelmények lehető legnagyobb mértékben történő teljesítésére.

# III. Adminisztratív védelmi intézkedések

Az ebben a fejezetben leírt adminisztratív védelmi intézkedéseket egységesen kell, valamennyi elektronikus információs rendszerre vonatkozóan megvalósítani.

## 8. Szervezeti biztonság

### 8.1. Információbiztonsági tevékenységek

A Hivatalban a következő információbiztonsági tevékenységeket kell ellátni:

a) informatikai kockázatelemzés és kezelés,

b) elektronikus információs rendszerek biztonsági felügyelete,

c) új elektronikus információs rendszerek információbiztonsági véleményezése és elfogadása,

d) szervezetek közötti információbiztonsági együttműködés,

e) az információbiztonság független felülvizsgálata.

### 8.2. Az információbiztonsági felelősségi rend meghatározása

Az információbiztonság megteremtése és fenntartása olyan alapvető felelősség, amely szerint nem tartozhat egyszemélyi felelősségi és hatáskörbe az elektronikus információs rendszerek tervezése, fejlesztése, üzemeltetése és felügyelete.

Az információbiztonság megvalósítását, fenntartását és ellenőrzését a Hivatal a feladatok és felelősség szempontjából egymástól elhatárolt szervezeti keretek között valósítja meg.

A Hivatal információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

a) a jegyző,

b) az információbiztonsági felelős,

c) a rendszergazda,

d) az adatgazdák,

e) a szervezeti egység vezetője,

f) a felhasználók.

## 8.3. A jegyző

A jegyző az Ibtv. alapján gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

### 8.3.1. A jegyző feladatai

A jegyző

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a Hivatalra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

c) az elektronikus információs rendszer biztonsági osztálya és a Hivatal biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel,

d) meghatározza a Hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az információbiztonsági szabályzatot,

e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról,

f) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Hivatal elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

h) 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,

i) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

j) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a jelen IBSZ-ben foglaltak szerződéses kötelemként teljesüljenek,

k) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

A jegyző köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során

a) az IBF személyéről tájékoztatást nyújt,

b) a Hivatal információbiztonsági szabályzatát tájékoztatás céljából megküldi,

c) megküldi a Hivatal elvárt biztonsági szintjének és az elektronikus információs rendszereinek elvárt biztonsági osztályának elérésére készített cselekvési tervet,

d) biztosítja a jogszabályokban meghatározott hatóságok részére az ellenőrzés lefolytatásához és a biztonsági incidensek kivizsgálásához szükséges feltételeket.

### 8.3.2. A jegyző felelőssége

A jegyző felelős a Hivatalban az Ibtv. által előírt biztonsági szintnek és biztonsági osztályoknak megfelelő információbiztonsági intézkedések megvalósulásáért.

## 8.4. Az IBF

A jegyző által megbízott IBF-nek a következők a feladatai, felelősségei és felelősségei:

### 8.4.1. Az IBF feladatai

Az IBF a Hivatal információbiztonsági irányítási rendszerének működtetése és ellenőrzésével kapcsolatos feladatai a következők:

a) gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a Hivatal elektronikus információs rendszereire vonatkozó információbiztonsági politikát, információbiztonsági stratégiát és az információbiztonsági szabályzatot,

d) intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához, ebben mérföldköveket határoz meg, azokat meghatározott időközönként felülvizsgálja, valamint karbantartja az intézkedési tervet,

e) előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe történő besorolását,

f) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit,

g) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Az IBF biztosítja a jogszabályokban meghatározott követelmények teljesülését

a) a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a Hivatal adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők,

az IBSZ hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

### 8.4.2. Az IBF jogai

Az IBF a Hivatal információbiztonságának fenntartása érdekében, illetve információbiztonsági incidens esetében jogosult:

a) külön engedély nélkül a Hivatal bármely helyiségébe belépni, amennyiben ott az információbiztonságot érintő munkavégzés folyik,

b) bármelyik számítógép, adathordozó vagy számítógépes lista tartalmába betekinteni, függetlenül annak minősítésétől (a vonatkozó jogszabályok betartásával), amennyiben az adott ügyben, illetve témában vizsgálat folyik,

c) minden értekezleten részt venni, észrevételeit és javaslatait megtenni, amelynek számítástechnikai, illetve információbiztonsági vonatkozása van, és ez az értekezlet összehívásakor ismert.

### 8.4.3. Az IBF felelőssége

Az IBF felelős a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.

## 8.5. A rendszergazda

A rendszergazda információbiztonsággal kapcsolatos feladata és kötelessége a következő:

### 8.5.1. A rendszergazda feladata

A rendszergazda feladata, hogy

a) az IBF-fel közösen meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket;

b) kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat,

c) biztosítja a rendszerfelügyeletet;

d) üzemelteti a rá bízott elektronikus információs rendszereket;

e) vezeti az IBSZ-ben előírt nyilvántartásokat.

f) gondoskodik a jelen IBSZ *{2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* mellékletében felsorolt elektronikus információs rendszerek naprakész nyilvántartásáról.

### 8.5.2. A rendszergazda felelőssége

A rendszergazda felelőssége az általa a jelen IBSZ *{2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* mellékletében felsorolt elektronikus információs rendszerek jelen IBSZ-ben foglaltak szerinti biztonságos üzemeltetése.

## 8.6. Az adatgazda

Az adatgazda annak az önálló szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését vagy nyilvántartás vezetését elrendeli.

Az adatgazdák a jelen IBSZ *{2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* mellékletében kerültek kijelölésre.

### 8.6.1. Az adatgazda feladatai

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

a) meghatározza az adatokhoz / tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges;

### 8.6.2. Az adatgazda felelőssége

Az adatgazda felelős a hatáskörébe tartozó elektronikus információs rendszerek hozzáférési jogosultságainak - a lehetőségek szerint - a „szükséges, minimális jogosultságok” elve alapján történő engedélyezéséért.

## 8.7. A szervezeti egység vezetője

A szervezeti egység vezetőjének feladata és felelőssége, hogy az általa irányított szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági előírásokat.

## 8.8. Önkormányzati ASP adminisztrátor

Az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat, intézmény, nemzetiségi önkormányzat) szintű felhasználó kezelés, azaz

a) az adott tenant felhasználóinak felvétele és szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása;

b) intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, illetve a tanúsítványokat hordozó tokenek csoportos átvétele és felhasználók közötti kiosztása.

## 8.9. Önkormányzat szakrendszeri adminisztrátor

Az önkormányzat szakrendszeri adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

## 8.10. A felhasználó

A Hivatal felhasználóinak az elektronikus információs rendszerek biztonságával kapcsolatban a következők a jogai, a kötelességei és a felelőssége:

### 8.10.1. A felhasználó jogai

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára,

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére,

c) információbiztonsági képzésre,

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni,

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

### 8.10.2. A felhasználó kötelessége

Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.

Valamennyi felhasználó köteles azonnal értesíteni felettesét a következő eseményekről, körülményekről:

a) az informatikához kapcsolódó tevékenység fennakadása, megszakadása,

b) ha olyan adatokhoz fér hozzá, melynek kezelésében nem illetékes,

c) információbiztonsági esemény.

Az munkahelyi vezetőnek jeleznie kell a tapasztaltakat a rendszergazda részére, aki információbiztonsági incidens esetén értesíti az IBF-et.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

### 8.10.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a jelen IBSZ *{7. sz. melléklet – Felhasználói Informatikai Biztonsági Házirend}* mellékletének megismeréséért és az abban foglalt szabályok betartásáért,

b) az önkormányzati ASP központ működtetője által közzétett felhasználói biztonsági követelmények betartásáért,

c) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért,

d) a személyre szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért,

e) az elektronikus információs rendszerben végzett műveletekért,

f) a Hivatal elektronikus információs rendszereinek szakszerű kezeléséért és

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

# 9. Személyi biztonság

## 9.1. A munkaköri felelősség és az alkalmazás feltételei

A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket.

A Hivatalnak tájékoztatnia kell a dolgozókat arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége arra az esetre is vonatkozik, ha nem a Hivatalban (pl. otthon), illetve a normál munkaidőn kívül dolgozik.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák az IBSZ előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *{8. sz. melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat és az ASP titoktartási nyilatkozat aláírása után lehet használatba venni.

## 9.2. Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal az információbiztonsági szempontból kulcsfontosságú munkaköröket és az azok betöltéséhez szükséges feltételeket meghatározta, ezek a következők:

| **Munkakör** | **Munkakör betöltéshez szükséges feltételek** |
|---|---|
| Helyi rendszergazda | Erkölcsi bizonyítvány, szakirányú végzettség, 2 év szakmai tapasztalat, alapfokú angol nyelvtudás |
| Információbiztonsági felelős | Erkölcsi bizonyítvány, szakirányú végzettség, 5 év szakmai tapasztalat, alapfokú angol nyelvtudás |
| Adatgazda | Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság |
| Önkormányzati ASP adminisztrátor | Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság |
| Önkormányzati szakrendszeri adminisztrátor | Erkölcsi bizonyítvány, szakirányú végzettség, informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság |
| Felhasználó | Erkölcsi bizonyítvány, szakirányú végzettség, |

| | |
|---|---|
| | informatikai alapismeretek, önkormányzati szakrendszerek használatában szerzett jártasság |

## 9.3. A személyek ellenőrzése

A Hivatal személyügyekért felelős vezetőjének a feladata, hogy az elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrizze, hogy az érintett személy a *{9.2. Munkakörök, feladatok biztonsági szempontú besorolása}* fejezetben meghatározott feltételeknek megfelel-e. A vizsgálat magában foglalja az alábbiakat:

*Biztonsági események jelentése}* a) referenciák ellenőrzése,

b) a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,

c) a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,

d) nyelvtudást igazoló okiratok ellenőrzése,

e) hatóság által kibocsátott azonosító irat ellenőrzése,

f) erkölcsi bizonyítvány ellenőrzése.

Külső szerződő felek esetében az IBF feladata az előzetes ellenőrzés elvégzése.

A munkaköri leírásokban rögzíteni kell a felelősségi köröket.

## 9.4. Az információbiztonság oktatása és képzése

A Hivatal elektronikus információs rendszereit csak olyan személyek használhatják, akik megfelelő számítástechnikai, informatikai ismeretekkel rendelkeznek.

Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

Új dolgozó munkába lépésekor a dolgozóval a munkába állás előtt az információbiztonsági előírásokat meg kell ismertetni. Ennek végrehajtására évente frissítő oktatást kell szervezni.

Az önkormányzati ASP szakrendszerek felhasználóinak az ASP működtetője által biztosított e-learning képzésen kell részt venni a szakrendszerhez történő hozzáférés előtt.

A kiemelt jogosultságokkal rendelkező munkatársak részére külön oktatást kell tartani.

Az információbiztonsági oktatások és továbbképzések tematikájának kidolgozása, a szükséges szakirodalom és tájékoztató anyagok biztosítása, valamint a képzés megtartása az IBF feladata.

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

## 9.5. Jelentés a biztonsági eseményekről

Dokumentált eljárást kell kialakítani a biztonsági eseményekről szóló jelentések elkészítésére, a visszajelzések kezelésére.

A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és az IBF-et.

Amennyiben a biztonsági esemény érinti az önkormányzati ASP rendszer által nyújtott szolgáltatásokat vagy közvetlenül azokban következik be, az eseményt jelenteni kell az önkormányzati ASP rendszer működtetőjének is.

A biztonságot érintő eseményekről szóló jelentések elkészítésére a jelen IBSZ *{3. sz. melléklet –* mellékletében található űrlapot kell használni.

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.

## 9.6. Jelentés a biztonság gyenge oldalairól

A rendszergazda köteles azonnal jelenteni az IBF-nek, amennyiben munkája során biztonsági veszélyeket, vagy az elektronikus információs rendszerben valamilyen gyenge pontot fedeztek fel.

A biztonságot érintő gyenge pontokról szóló jelentések elkészítésére a jelen IBSZ *{3. sz. melléklet – Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

## 9.7. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

g) fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet is,

h) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből. A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Abban az esetben, hogy ha feltételezhető az információbiztonság sérülése, akkor az eseményt
a rendszergazda jelenti az IBF-nek, aki a jelen *IBSZ {3. sz. melléklet – Biztonsági események jelentése}* pontjának megfelelően kivizsgálja az eseményt.

## 9.8. Okulás a biztonsági eseményekből

Az IBF-nek a bejelentett biztonsági eseményekről, veszélyes helyzetekről, illetve a működési zavarokról, azok előfordulási gyakoriságáról, és kezelésükre tett intézkedések eredményéről háromhavonta jelentést kell készítenie jegyző számára.
Az IBF feladata a biztonsági események kezelése során nyert tapasztalatok felhasználásával a meglévő biztonsági rendszer – így a szabályozó elemek és technikai megoldások felülvizsgálata és szükség esetén tökéletesítése.
Szükség esetén (nagy kár, vagy várható jelentős potenciális kár, illetve gyorsan szaporodó előfordulás esetén) az egyes eseményeket, az illetve esemény típusokat IBF-nek soron kívül jelentenie kell a jegyző részére.

## 9.9. Munkavállalói jogviszony megszűnésekor

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

a) Jogosultságok megszüntetése, úgy hogy a régi állapot mentésre vagy dokumentálásra kerül.

b) A felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról.

c) Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve ha szükséges a megadott idő után törölni a rendszerből.

A fenti feladatok végrehajtásáért a rendszergazda a felelős.

## 9.10. Vagyontárgyak visszaszolgáltatása

Valamennyi felhasználónak, a szerződőknek és a felhasználó harmadik félnek vissza kell szolgáltatnia a Hivatal valamennyi használatra átvett vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

A rendszergazdának az eszköz leadásakor ellenőriznie kell, hogy a felhasználó az átvételi elismervényben rögzített hardver-, szoftver specifikációval adja-e vissza a munkaállomást.

## 9.11. Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és a felhasználó harmadik feleknek információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár.

A feladatok végrehajtásáért a rendszergazda a felelős.

Az ASP szakrendszerek esetében az önkormányzati ASP adminisztrátor és az önkormányzat szakrendszeri adminisztrátor feladata, hogy intézkedjen a jogosultságok megszűntetéséről a működtető felé.

## 9.12. Információbiztonsági kötelmek a munkavállalói jogviszony megszűnése után

A személyügyi referensnek a jelen IBSZ *{9. sz. melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén}* mellékletében foglaltak szerint tájékoztatnia kell a dolgozót arról, hogy a jelen IBSZ-ben foglalt kötelezettségei a jogviszony megszűnése után is fennállnak, az abban foglaltak megsértése jogi következményeket von maga után.

## 9.13. Fegyelmi intézkedések

A szabályok megszegéséről az észlelő haladéktalanul köteles tájékoztatni az IBF-et. Az IBF a tudomására jutott események súlyosságát mérlegeli, és szükség esetén jelenti a jegyzőnek.

A biztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor.

## 9.14. Harmadik felekkel kapcsolatos előírások

Harmadik fél csak egyedi esetben, meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal, amit szerződésben kell dokumentálni. A hozzáférést az elektronikus információs rendszer adatgazdájának kell engedélyezni.

A Hivatal és szerződéses partnerei megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

A harmadik félnek a Hivatal elektronikus információs rendszereihez történő hozzáférése esetében - figyelembe véve a szükséges hozzáférési típusokat, az információ értékét, a harmadik fél által alkalmazott biztosítékokat, valamint a hozzáférés mélységét - törekedni kell a kockázatok minimalizálására.

Azokban az esetekben, amelyekben az információ feldolgozása vagy kezelése kiszervezéssel történik, a harmadik féllel kötött szerződésnek a betartandó biztonsági követelményeket is tartalmaznia kell.

Harmadik fél hozzáférése a Hivatal adataihoz és információihoz, a munkájához elengedhetetlenül szükséges minimum szintre kell korlátozni. A hozzáférések feltételeit szerződésben kell részletezni. A szerződés csak a Hivatal jelen IBSZ-évelösszhangban lévő követelményeket tartalmazhat.

A szerződésnek tartalmaznia kell továbbá a bizalmasságra, a szellemi tulajdonjogokra, a szerzői jogok átruházására és minden közösen végzett munkálatok védelmére vonatkozó nem nyilvános garanciákat is.

A szerződésben elő kell írni, hogy a Hivatal információs vagyonelemei a szerződés lejártát követően kerüljenek vissza a Hivatal birtokába, a szerződött félnél - valamint annak partnereinél, alvállalkozóinál - pedig kerüljenek megsemmisítésre.

A szerződéses partnernek a Hivatallal egyeztetnie kell a számára nyújtott szolgáltatásokkal kapcsolatos minden részdöntést.

A szerződésben a Hivatal számára jogot kell biztosítani arra, hogy a már kölcsönösen elfogadott szerződéses felelősséget felülvizsgálja, szükség esetén harmadik féllel felülvizsgáltassa.

Harmadik fél a Hivatal adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés és a jelen IBSZ *{10. sz. melléklet – Titoktartási Nyilatkozat}* mellékletében található titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

### 9.14.1. A harmadik fél hozzáférési kockázatának azonosítása

A Hivatalnak fel kell mérnie, és meg kell határoznia, hogy mekkora a kockázata annak, ha a harmadik félnek hozzáférési joga van a Hivatal információs vagyonához.

A kockázatok felmérése a jelen IBSZ *{4. sz. melléklet – Kockázatelemzési és kezelési módszertan}* melléklete szerint történik. A kockázatkezeléshez, a megfelelő óvintézkedések kialakításához és a hozzáférések engedélyezéséhez a hozzáférés igénylésben pontosan meg kell határozni a hozzáférések típusát és azt, hogy milyen okból történik a hozzáférés.

A kockázat meghatározásért a harmadik féllel kötött szerződés teljesítésében elsődlegesen érintett szervezeti egység vezetője a felelős, és a szerződés megkötése előtt köteles az informatikai biztonsági felelőst bevonni a szerződéskészítés folyamatába.

### 9.14.2. A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, szükség esetén az alábbiakat kell figyelembe venni:

a) az informatikai biztonság fő szabályait;

b) az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat;

c) az információk másolásának és nyilvánosságra hozatalának feltételeit;

d) a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;

e) a felek felelősségének meghatározását;

f) a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;

g) a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

h) a felmerülő problémák kezelését;

i) a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;

j) világos és egyértelmű jelentéskészítési struktúrát és rendszert;

k) a változáskezelések egyértelmű és meghatározott folyamatát;

l) óvintézkedések meghatározását a kártékony kódok ellen;

m) biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;

n) az alvállalkozók bevonására vonatkozó szabályokat.

Abban az esetben, ha a feladat elvégzésére a harmadik fél alvállalkozót is igénybe vesz, a szerződésben pontosan meg kell nevezni az alvállalkozót, s meg kell határozni a rá vonatkozó hozzáférési jogosultságokat. A titoktartási kötelezettség a harmadik fél alvállalkozójára is vonatkozik, és a szerződésnek titoktartási nyilatkozat részt is kell tartalmaznia.

## 10. Az elektronikus információs rendszerek nyilvántartása

Nyilvántartást kell vezetni az általa működtetett valamennyi elektronikus információs rendszerről. A nyilvántartásnak minden elektronikus információs rendszerre nézve a következőket kell tartalmaznia:

a) annak alapfeladatait;

b) a rendszerek által biztosítandó szolgáltatásokat;

c) az érintett rendszerekhez tartozó licenc számot;

d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

e) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A nyilvántartást a rendszergazdának kell vezetnie.

## 11. Kockázatelemzés és kezelés

Az információbiztonsági kockázatelemzés célja, hogy feltárja a Hivatal elektronikus információs rendszereire és az azokban kezelt adatokra ható fenyegető tényezőket, veszélyforrásokat (fenyegetettség elemzés), vizsgálja az elektronikus információs rendszer

gyenge pontjait (sérülékenység vizsgálat), elemezze a veszélyforrások által a gyenge pontokon keresztül bekövetkező sikeres támadások bekövetkezési valószínűségét és az általuk okozott kár nagyságát (kockázatelemzés), valamint kezelje a Hivatal által el nem fogadható kockázatokat (kockázatkezelés).

A kockázatarányos védelem kialakításához rendszeres és tervszerű informatikai kockázatkezelésre van szükség. Annak érdekében, hogy a kockázatkezelési folyamata a Hivatal számára jól követhető, megismételhető és ellenőrizhető legyen, írásos kockázatkezelési módszertanra van szükség, mely mind a kockázatelemzés, mind a kockázatkezelés területén lefekteti az alapvető végrehajtási módszereket.

A Hivatal kockázatelemzési és kezelési eljárásrendjét az *{4. sz. melléklet – Kockázatelemzési és kezelési módszertan}* tartalmazza.

### 11.1. Kockázatelemzés

A kockázatarányos védelem kialakításához rendszeres és tervszerű informatikai kockázatelemzésre van szükség. A kockázatelemzést a jelen IBSZ *{4. sz. melléklet – Kockázatelemzési és kezelési módszertan}* mellékletében leírt módszertan alapján az IBF végzi el.

A kockázatelemzést évente el kell végezni, melynek során felül kell vizsgálni az előző évi kockázatelemzés eredményét. A kockázatelemzést soron kívül el kell végezni, hogy ha

a) változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését),

b) olyan körülmények következnek be, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát.

A kockázatelemzés eredményét IBF-nek dokumentálnia kell, majd meg kell ismertetnie a jegyzővel.

A nem tolerálható kockázatok kezelésére intézkedési tervet kell készíteni, melynek tartalmaznia kell a kockázat kezelésére javasolt intézkedéseket, felelős, határidő és költségvonzat megjelölésével.

A kockázatkezelési tervet az IBF-nek kell előkészítenie és a jegyző hagyja jóvá.

A kockázatelemzéssel és kezeléssel kapcsolatos dokumentumok bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

## 12. Tervezés - Biztonságtervezési eljárásrend

### 12.1. Rendszerbiztonsági terv

El kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, mely a következőket tartalmazza:

a) az elektronikus információs rendszer hatóköre, alap feladatai (biztosítandó szolgáltatásait), biztonságkritikus elemei és alap funkciói,

b) az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztálya,

c) az elektronikus információs rendszer működési körülményei és más elektronikus információs rendszerrel való kapcsolatai.

Az elektronikus információs rendszer biztonsági követelményeit a vonatkozó rendszerdokumentációban kell rögzíteni.

Meg kell határozni a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedésbővítéseket, illetve végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

A rendszerbiztonsági tervet meg kell ismertetni a Hivatal érintett munkatársaival illetve a fejlesztővel.

Az elektronikus információs rendszerek rendszerbiztonsági tervét kétévente felül kell vizsgálni.

Soron kívül felül kell vizsgálni a rendszerbiztonsági terveket az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

Az elektronikus információs rendszerek rendszerbiztonsági tervét az érintettek bevonásával az IBF készíti el.

A rendszerbiztonsági tervek bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

## 12.2. Az internet használat és az elektronikus levelezés szabályai

A Hivatal által nyújtott internetkapcsolat és elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai.

### 12.2.1. A web böngészés szabályai

Az Internethez való kapcsolódás elsődlegesen a munkavégzést szolgálja!

Az Internet és az elektronikus levelezés használatának főbb szabályai:

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az rendszergazda jelentést tesz az IBF-nek, aki eljár az ügyben a jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi illetve jogellenes tevékenységre.

Az internetről csak Hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

### 12.2.2. E-mail használat

A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a Hivatali e-mail címüket nem hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

Elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására.

A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.

Zavaró, félreinformáló levelek, spam-ek küldése, jogtalan megrendelések elindítása tilos, és eljárást vonhat maga után.

Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ezeket olvasatlanul törölni kell.

## 13. Rendszer és szolgáltatás beszerzés

A Hivatal saját hatókörében informatikai szolgáltatást, vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet.[2]

# IV. Fizikai védelmi intézkedések

## 14. Alapelvek

Az elektronikus információs rendszer fizikai környezetének kialakítása, működtetése és használata során az általános biztonsági előírások szerint kell eljárni, az alábbiak szerint:

a) az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni, és a környezetet a berendezések gyártói által megadott fizikai feltételek szerint kell kialakítani, fenntartani;

[2] Ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket. Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése. (Lásd technológiai vhr 4. sz. melléklet 3. 1.4.1. pontja

b) a környezeti fizikai feltételeket (hőmérséklet, páratartalom, áramszolgáltatás stb.) folyamatosan ellenőrizni kell;

c) a megbízható működés biztosítása céljából a körülményeknek megfelelő legfontosabb klímatechnikai, épületgépészeti, áramellátó tartalékberendezésekről gondoskodni kell.

# 15. A területek fizikai biztonsági követelményei

## 15.1. Fizikai biztonság védősávja

A védett helyiségeket, illetve területeket a fenyegetettség és kockázat mértéke szerint biztonsági zónákba kell besorolni. Héjszerű, többlépcsős fizikai védelmet kell kialakítani.

A jelen IBSZ *{2.2 Tárgyi hatály}* pontja alá eső területeket az alábbi kategóriák egyikébe kell besorolni:

a) belső terület;

b) védett terület;

c) érzékeny terület.

További védett terület kategóriákat az IBF határozhat meg.

## 15.2. Belső terület

Belső területnek tekintendők a Hivatal bejárata utáni közös használatú helyiségei és folyosói.

A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az IBF feladata.

## 15.3. Védett terület

Védett terület valamennyi helyiségeit nem szabad őrizetlenül hagyni.

A védett területek helyiségeinek elhagyásakor a munkaállomásokat zárolni kell. Munkaidőn kívül a védett területek helyiségeit a hivatal épületének általános riasztó rendszerével kell védeni.

## 15.4. Érzékeny terület

Érzékeny terület a Hivatal elektronikus információs rendszereket koncentráltan tartalmazó helyiségei.

Látogatók belépése az érzékeny területre csak hivatalos célból, ellenőrzötten és kísérővel történhet. A látogatóknak a figyelmét fel kell hívni az érvényben lévő biztonsági előírásokra.

Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében belépési naplót kell vezetni.

A belépési naplót a jegyzői titkárságon kell tárolni.

Az érzékeny területek elérésére a jegyző, a rendszergazda és az IBF jogosultak. Minden más személy részére csak a jegyző engedélyezheti a belépést az érzékeny területekre.

Az érzékeny területek belépési naplóit, valamint a kiosztott jogosultságokat az IBF-nek havi rendszerességgel ellenőriznie kell.

### 15.5. Az irodák, a helyiségek és az eszközök védelme

A Hivatalnak az irodák, a szobák és a számítógépterem védelmét az alábbiak szerint kell szabályozni:

a) a védett és érzékeny helyiségek átlagos kinézetűek legyenek, ne hívják fel magukra a figyelmet, ne legyen rajtuk olyan jelzés, amelyből kiderül a funkciójuk;

b) a fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni;

c) a dokumentumok tárolása védettszekrényekben történjen;
d) Személyes adatokat tartalmazó iratokat csak zárható helyen szabad tárolni.

### 15.6. Munkavégzés biztonságos környezetben

Az érzékeny területeken dolgozó és az ideiglenes jellegű munkát végző harmadik félre vonatkozóan elő kell írni, hogy számukra a hozzáféréseket csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani. A hozzáférések szabályait előzőleg az IBF-nek jóvá kell hagynia.

## 16. Az infokommunikációs eszközök biztonsága

Az információs vagyon - lopás, veszélyeztetés, egyéb károsodás elleni - védelmének és a működési folyamatok folytonosságának biztosítása érdekében a Hivatal infokommunikációs eszközeit, azok megfelelő fizikai elhelyezésével és kezelésével is biztosítani kell.

### 16.1. Az infokommunikációs eszközök elhelyezése és védelme

Az infokommunikációs eszközöket úgy kell elhelyezni, és védelmüket úgy kell kialakítani, hogy minimálisra csökkenjenek a környezeti hatások következtében megjelenő kockázatok, és minimálisra csökkenjen az illetéktelen hozzáférések lehetősége, de a munkavégzés hatékonysága ne romoljon.

A védelmi intézkedések biztosítsák, hogy a különböző környezeti hatás miatt keletkező meghibásodások csökkenjenek. Ezért:

a) be kell tartani a tűzvédelmi előírásokat;

b) a Hivatal területére a normál háztartási vegyi anyagokon, tisztítószereken túl vegyi anyagot, robbanóanyagot behozni tilos;

c) a monitorokat úgy kell elhelyezni, hogy ki lehessen zárni azok illetéktelen leolvasását;

d) Különös figyelmet kell fordítani az önkormányzati ASP rendszert elérő munkaállomások elhelyezésére, gondoskodni kell az illetéktelen hozzáférések megakadályozásáról.

## 16.2. Tápáramellátás

A kritikus infokommunikációs eszközök (kiszolgáló, tűzfal, router, switch) működését szünetmentes áramforrásról kell biztosítani. Intézkedéseket kell foganatosítani, hogy a kiszolgálók az áthidalási időn belül szabályosan leállíthatók legyenek.

## 16.3. A kábelezés biztonsága

Biztosítani kell az elektromos és adatvezetékek megszakadás és a rongálások elleni megfelelő védelmét.

A hálózati zavarok okozta hibák elkerülése érdekében az erősáramú vezetékeket el kell különíteni a kommunikációs hálózattól. A kábelstruktúra legyen érzéketlen az elektromos hálózati zavarokra.

## 16.4. „Üres asztal - üres képernyő" szabály

Az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden dolgozónak ismernie és alkalmaznia kell a jelen pontban leírtakat:

a) a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);

b) a felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) a zárolás elfelejtésének esetére jelszóvédett, automatikus zárolást kell beállítani, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

d) a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a munkaállomást;

e) ügyfelet irodában felügyelet nélkül hagyni tilos.

## 16.5. Felügyelet alól kikerülő eszközök

Szerviz részére eszközt csak a rendszergazda adhat át. Szervizbe történő szállítás esetén a szerviz által adott szállítólevelet a rendszergazda őrzi meg.

Szervizbe történő szállításkor vagy garanciális javítás esetén - jegyzőkönyv felvétele mellett – a rendszergazdának gondoskodnia kell az adatokat tartalmazó adathordozók törléséről.

A munkatársak részére hosszú távú használatra kiadott nagy értékű eszközökről (pl.: laptop) a Hivatalnak nyilvántartást kell vezetnie. Ezen eszközöket a munkatársak korlátozás nélkül ki-és beszállíthatják.

Minden más esetben eszközt kiszállítani csak a rendszergazda írásos engedélyével lehet.

A ki- és beszállítások ellenőrzése a rendszergazda feladata. Infokommunikációs eszközök és berendezések írásos engedély nélküli ki- és beszállításának kísérlete esetét jelenteni kell az IBF-nek a szabálysértést elkövető személy felettes vezetőjének egyidejű értesítése mellett.

Az információbiztonsági tudatosság fokozását célzó oktatások keretében a felhasználókat tájékoztatni kell az ezzel kapcsolatos ellenőrzési feladatokról és jogokról.

## 17. Fizikai belépési engedélyek

A Hivatalnak össze kell állítania azon személyek listáját, akik jogosultak a védett és az érzékeny területekre történő belépésre.

A listát a jegyző hagyja jóvá.

Az IBF évente vagy személyi változás esetén ellenőrzi a belépésre jogosult személyek listáját és eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése már nem indokolt.

# V. Logikai védelmi intézkedések

A logikai védelmi intézkedések a technológiai vhr alapján kerültek kialakításra.

A jelen IBSZ *{2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása}* melléklete alapján megállapítható, hogy a Hivatalnak nincsen 2-es biztonsági osztálynál magasabb elektronikus információs rendszere, ezért a jelen fejezetben előírt követelmények a 2-es biztonsági osztályra vonatkoznak.

## 18. Konfigurációkezelési eljárásrend

### 18.1. Alap konfiguráció

A Hivatal valamennyi elektronikus információs rendszeréhez elkészíti az alapkonfigurációt, amelyet dokumentált formában biztonságos helyen tárolni szükséges.

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia:

a) Hardver elemek;

b) Szoftverek;

c) Telepítőkészletek;

d) Egyes szoftverkomponensek alapkonfigurációi.

Az egyes elektronikus információs rendszerek alapkonfigurációját a rendszergazda hathavonta felülvizsgálja, és a módosításokat átvezeti.

### 18.2. Elektronikus információs rendszerelem leltár

Az elektronikus információs rendszerek valamennyi hardver/szoftver eleméről a rendszergazdának nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a kiszolgálók és munkaállomások pontos és naprakész hardver konfigurációját, az elhelyezkedésüket, a működő alkalmazások egyedi beállításait és az értük felelős személy nevét.

### 18.3. A szoftver használat korlátozásai

A Hivatalban kizárólag a jegyző által engedélyezett, jogtiszta, a megfelelő licence-el rendelkező szoftvereket lehet használni.

Az alkalmazott szoftverekről leltárt kell vezetni.

Szabad vagy nyílt forráskódú szoftverek használatbavételét a jegyző engedélyezi. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell.

A másolatok és szétosztások ellenőrzése érdekében a telepítőkészleteket és a licenceket tartalmazó dokumentumokat páncélszekrényben kell tárolni és a hozzáféréseket ellenőrizni kell.

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

### 18.4. 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.

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróbaszerűen ellenőrzi.

## 19. Elektronikus információs rendszerek ügymenet folytonosságának tervezése

A Hivatal elektronikus információs rendszereinek folyamatos működésének biztosítása érdekében, valamint a katasztrófa-helyzetek bekövetkezte során a jelen fejezetben foglaltak szerint kell eljárni.

Az önkormányzati ASP rendszer által nyújtott szolgáltatások ügymenet-folytonosságának a biztosítása a működtető feladata.

### 19.1. Ügymenet folytonosságra vonatkozó eljárásrend

Az IBF-nek az érintett területek bevonásával ki kell dolgoznia és jóvá kell hagyatnia az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet (továbbiakban: ÜFT).

A folyamatos működés tervezésére vonatkozó tevékenységeket össze kell hangolni a biztonsági események és vészhelyzeti/katasztrófa helyzetek kezelésével.

A tervezés során meg kell határozni a Hivatal által biztosítandó szolgáltatásokat és alapfunkciókat, valamint az ezekhez kapcsolódó és a Hivatal részéről elvárt vészhelyzeti követelményeket.

Meg kell határozni az elektronikus információs rendszer kiesése esetére a helyreállítási feladatokat, a helyreállítási prioritásokat és azok mértékét.

Ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket.

Az ügymenet-folytonosságot úgy kell kialakítani, hogy az biztosítsa a Hivatal által előzetesen definiált alapszolgáltatások fenntartását, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

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

### 19.1.1. Az ÜFT felülvizsgálata

Az Ügymenet-folytonossági tervet évente felül kell vizsgálni.

Az Ügymenet-folytonossági tervet soron kívül felül kell vizsgálni

a) az elektronikus információs rendszer vagy a működtetési környezet jelentős változása,

b) az ügymenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémák esetén.

Az Ügymenet-folytonossági terv változásairól képzés formájában tájékoztatni kell az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.

### 19.1.2. Az ÜFT kezelése

Az Ügymenet-folytonossági terv jóváhagyott példányának páncélszekrényben történő őrzéséről a rendszergazda gondoskodik.

Az Ügymenet-folytonossági terv bizalmas dokumentumnak tekinthető, ezért csak az abban megjelölt személyek számára hozzáférhető, illetékteleneknek nem adhatják tovább.

## 19.2. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jog-szabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárás-rendet kell kidolgozni a következők figyelembevételével:
Rendszeres mentéseket kell készíteni a legalább 2-es biztonsági osztályba sorolt elektronikus információs rendszerekről és az azokban kezelt adatokról. A mentések során a következő adat-fajták mentését kell biztosítani:

a) felhasználói szintű adatok (ügyviteli adatok)

b) rendszerszintű információk

c) a rendszerrel kapcsolatos dokumentációk.

Biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a lényeges adatok és szoftverek esetleges adathordozó hiba, az elektronikus információs rendszerek összeomlása vagy meg-semmisülése esetén visszaállíthatóak legyenek. A mentési eljárásrendet úgy kell kialakítani, hogy az egyrészt megfeleljen az üzembiztonsági elvárásoknak, másrészt minél biztonságosabb védelmet nyújtson az esetlegesen előforduló hibák ellen. Az alkalmazások fizikai védelme érdekében, gondoskodni kell arról, hogy a telepítő állományok ne károsodjanak, ezért az eredeti példányukról biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tá-rolni. Az eredeti hordozókról készített másolatokat kell a napi tevékenység során használni. Az olvasási biztonság fenntartása érdekében az eredeti adathordozókról rendszeres időközönként frissítő mentést kell készíteni.
A rendszerek 466/2017. (XII. 28.) Korm. rendeletnek megfelelő adattrezorban való archiválása a Kormányzati Felhő üzemeltetője (a rendszer mindenkori adatkezelője) által történik

## 19.3. Az elektronikus információs rendszer helyreállítása és újraindítása

Az ügymenet-folytonosság tervezése során ki kell dolgozni az elektronikus információs rendszerek helyreállítási terveit, melyek a katasztrófahelyzetek kezelésére vonatkozóan a következőket kell tartalmaznia:

a) katasztrófát követő helyreállítandó célállapot;

b) a katasztrófa események definíciója;

c) a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;

d) a helyreállítási terv hatóköre;

e) a megelőzés érdekében végzett tevékenységeket;

f) felkészülés a katasztrófa elhárítására;

g) katasztrófa esetén végrehajtandó tevékenységek;

h) elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot;

i) a helyreállítási terv tesztelése, karbantartása.

Az elektronikus információs rendszerekre vonatkozó helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terv készítési tevékenységeket az IBF-nek információbiztonsági szempontból támogatnia és rendszeresen ellenőriznie kell.

A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása).

A rendszergazdának - mindezeken túl - gondoskodnia kell az elektronikus információs rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.

## 19.4. Rendszer karbantartási eljárásrend

Az elektronikus információs rendszerek karbantartására vonatkozóan a jelen fejezetben leírtak az irányadók.

Az önkormányzati ASP rendszer szakrendszereinek rendszeres karbantartása a működtető feladata.

### 19.4.1. Rendszeres karbantartás

A folyamatos működés érdekében a Hivatal elektronikus információs rendszereit a gyártó ajánlása alapján rendszeresen karban kell tartani. A karbantartások ütemezése, végrehajtása és az ellenőrzés megszervezése a rendszergazda feladata.

### 19.4.2. A karbantartások engedélyezése

A tervezett karbantartásokat dokumentált formában a jegyző engedélyezi. Amennyiben ez az elektronikus információs rendszerek leállításával jár, akkor a felhasználókat a karbantartás megkezdése előtt legalább 1 héttel értesíteni szükséges.

### 19.4.3. A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani. A nyilvántartásba a következő adatokat kell minimálisan rögzíteni:

a) az elvégzett karbantartás megnevezése,

b) az érintett eszközök, szoftverek, elektronikus információs rendszerek,

c) a karbantartás engedélyezője,

d) a karbantartás elvégzője,

e) a karbantartás dátuma,

f) leállási idő (ha volt ilyen).

A jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz.

### 19.4.4. A karbantartások ütemezése

Éves karbantartási tervet kell készíteni, melyben meg kell tervezni a karbantartások ütemezését. A terv elkészítése a rendszergazda, a terv jóváhagyása a jegyző feladata.

### 19.4.5. Kiszállítás

Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor az *{20.2 Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása}* fejezetben leírtak szerint kell eljárni. A kiszállítást a rendszergazda engedélyezi.

### 19.4.6. A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.

### 19.4.7. Karbantartók

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor a rendszergazda kezdeményezi a jegyzőnél külső fél (alvállalkozó) megbízását.

Karbantartási tevékenységet csak olyan külső fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a Hivatal vonatkozó információbiztonsági előírásait.

A karbantartást végző külső felekről nyilvántartást kell vezetni, melynek minimálisan a következőket tartalmaznia:

a) szervezet megnevezése,

b) szerződésszám,

c) szerződés időtartama,

d) szerződéses kapcsolattartó neve, elérhetősége,

e) karbantartás végzők neve, elérhetősége,

f) szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külsős szerződő fél munkavégzése esetén a rendszergazdának ki kell jelölnie azokat a személyeket, akiknek folyamatos felügyeletet kell biztosítani a karbantartás során.

A külső féllel kötött szerződébe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

# 20. Adathordozók védelmére vonatkozó eljárásrend

Az adathordozók védelmére a következő előírások vonatkoznak.

## 20.1. Hozzáférés az adathordozókhoz, adathordozók használata

A Hivatalban csak a Hivatal tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a szervezeti egység vezetőjének.

Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot floppyn, CD-n, elektronikus levélben vagy egyéb más módon (Pl.: Pen drive) a Hivatal informatikai infrastruktúrájából kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazda szervezeti egység vezetőjének kell engedélyeznie, minden esetben írásos formában.

A Hivatal az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

## 20.2. Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása

Az infokommunikációs eszközök újrahasznosítása vagy mások rendelkezésre bocsátása előtt minden esetben gondoskodni kell arról, hogy az infokommunikációs eszközökön tárolt információk visszaállíthatatlanul eltávolításra kerüljenek. Ennek érdekében

a) a rajtuk tárolt adatokat törölni kell;

b) a törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia;

c) garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az IBF dönt az eszköz cserére történő kiadhatóságáról, vagy megsemmisítéséről.

Az adatok megfelelő módon történő eltávolításáért az adatgazda a felelős. Az adatok eltávolítását a rendszergazda végzi. Az adatok eltávolítását jegyzőkönyvezni kell.

## 20.3. Az infokommunikációs eszközök Hivatalon kívüli biztonsága

A Hivatal területén kívüli infokommunikációs eszközök használatát a legszükségesebb mértékűre kell korlátozni. Kizárólag a Hivatal tulajdonát képező hordozható infokommunikációs eszköz használata engedélyezhető.

### 20.3.1. A hordozható infokommunikációs eszközök védelme

A hordozható infokommunikációs eszközök használata során a munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;

b) cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek, emiatt nem szabad őrizetlenül hagyni autóban, szállodai szobában;

d) a mobil infokommunikációs eszközök ellopása esetén:

i. az ellopás tényét a lehető leggyorsabban jelenteni kell az IBF-nek;

ii. értesíteni kell a rendőrséget;

iii. értesíteni kell a szálloda vezetését, ha az eszközt a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

iv. valamennyi rendőrségi jelentést meg kell őrizni és a jegyző részére át kell adni.

Az Önkormányzati ASP rendszerhez hozzáférést biztosító E-személyi kezelésénél különös figyelmet kell fordítani a fentiek alkalmazására.

### 20.3.2. Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az IBF-nek, valamint tájékoztatni kell őket arról, hogy az eszköz tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

## 21. Azonosítási és hitelesítési eljárásrend

Az önkormányzati ASP rendszer által nyújtott szolgáltatások azonosításának és hitelesítésének a módját (hitelesítés módja, alkalmazott eszközök, jelszóházirend, fiókzárolás, munkamenetek kezelése) a működtető határozza meg.

### 21.1. Azonosítás és hitelesítés (szervezeten belüli felhasználók)

Valamennyi elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie a Hivatal valamennyi felhasználóját és a felhasználók által végzett tevékenységeket.

Ennek érdekében egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

### 21.2. Azonosító kezelés

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat a rendszergazda hozza létre. Az azonosítók ismételt felhasználása tilos.

45 nap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania.

A fentiek havi rendszerességgel történő végrehajtása az rendszergazdák feladata.

Az önkormányzati ASP szakrendszereihez történő csatlakozás többtényezős hitelesítéssel történik. A felhasználónak rendelkeznie kell E-személyi-vel, valamint kártyaolvasóval.

Az E-személyihez csak a hozzá tartozó PIN kód megadásával lehet hozzáférni. A PIN kód megadása után. A sikeres azonosítást és hitelesítést követően az ASP rendszer az egyes szakrendszerekhez történő hozzáférés során további azonosító adatokat (felhasználói név, jelszó) kérhet.

## 21.3. A hitelesítésre szolgáló eszközök kezelése

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.

A Hivatal jelszókezelő rendszere:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;

b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

c) kényszerítse ki a megfelelő minőségű jelszavak használatát;

d) kényszerítse ki a jelszóváltoztatást;

e) tiltsa meg a korábban használt jelszavak ismételt felhasználását;

f) beíráskor ne jelenítse meg a jelszavakat a képernyőn;

g) a jelszó állományokat rejtjelezve tárolja;

h) változtassa meg a szállító alapértelmezett jelszavát a szoftver installálása után.

Jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni, úgy, hogy:

a) szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;

b) biztosítani, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) a jelszó legalább nyolc karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat két napon belül nem szabad megváltoztatni;

c) az előző jelszavak újra használatát kerülni kell;

d) zárolás esetén előre beállított időtartam eltelte után engedélyezze vissza a felhasználói fiókot.

## 21.4. A felhasználó felelősségi köre a jelszó használat során

A Hivatal elektronikus információs rendszereiben a jelszavak használatának és képzésének részletes szabályai a következők:

a) a felhasználó a jelszavát köteles titokban tartani;

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben;

c) a felhasználói jelszót TILOS leírni;

d) ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni és értesíteni kell az IBF-et;

e) nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

f) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el. Ennek érdekében az alábbi szempontokat kell betartani:

g) könnyen megjegyezhető, és nehezen kitalálható legyen;

h) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

i) ne legyen a gépnévre vagy a felhasználói névre utaló;

j) ne legyen sorozat.

Különös figyelmet kell fordítani az E-személyihez tartozó PIN kód titokban tartására, mivel az E-személyi-vel minősített elektronikus aláírás hozható létre, mely teljes bizonyító erejű magánokiratnak megfelelő joghatással bír.

A fenti szabályok az elektronikus információs rendszerek által technikailag kikényszeríthető részét a rendszergazdának kell beállítani.

A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben.

## 21.5. Azonosító kezelés

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat a rendszergazda hozza létre. Az azonosítók ismételt felhasználása tilos. 2 hónap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania.

## 21.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az illetéktelen hozzáférések elkerülése érdekében olyan hitelesítési módszereket kell alkalmazni, amely a sikertelen bejelentkezési kísérletekről nem ad vissza semmilyen olyan érdemi információt, amelyet egy támadó ki tud használni és illetéktelenül hozzá tud férni a Hivatal elektronikus információs rendszereihez.

## 21.7. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie az érintett szervezeten kívüli felhasználókat, illetve a tevékenységüket.

## 21.8. Hitelesítés szolgáltatók tanúsítványának elfogadása

A Hivatal elektronikus információs rendszereihez az Internet irányából csak szabványos, kriptográfiai módszerrel azonosított és hitelesített felhasználó, titkosított hálózati kapcsolaton keresztül lehet hozzáférni.

A nem a hivatal állományában lévő felhasználó külső hozzáférése esetén a hálózati kommunikáció titkosításához csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

## 22. Hozzáférés ellenőrzési eljárásrend

A hozzáférési jogok kezelését jelen eljárásrendben foglaltak szerint kell megvalósítani a következő alapelvek alkalmazásával:

a) Minden felhasználó csak a feladatellátásához szükséges, minimális jogosultságot kapja meg.

b) A felhasználók a munkaállomásukon nem rendelkezhetnek rendszergazda jogokkal.

c) A rendszergazda a rendszerek adminisztrálásához használt adminisztrátori azonosítóját a napi munkavégzése során nem használhatja. A napi munkavégzéshez normál felhasználói jogú azonosítót kell használnia.

d) Az önkormányzati ASP szakrendszerekhez történő hozzáféréseket a működtető által megfogalmazott eljárásrend alapján kell kezelni.

### 22.1. Felhasználói fiókok kezelése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:

a) A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

b) Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.

c) Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

f) Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén, papír alapon kell a nyilvántartást vezetni.

g) Minden egyes elektronikus információs rendszerhez, csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.

h) Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

A felhasználók nyilvántartásba vételi szabályainak és a követendő eljárásrend kidolgozásakor a következőket kell figyelembe venni:

a) A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.

b) A csoportos felhasználó azonosítók használatát tiltani kell.

c) A felhasználói hozzáférési jogosultságokat a szervezeti egység vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:

i. a felhasználó munkakörét és az azzal kapcsolatos feladatait;

ii. a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;

iii. a felhasználó jogviszonyát;

iv. a felhasználó munkahelyét.

d) A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell: i.

a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;

ii. annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;

iii. azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör, vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;

iv. annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;

v. a munkahelyi vezető aláírását.

e) A jogosultságigénylési lapot az igényelt és a beállított jogosultságok egyeztetése céljából a rendszergazda tárolja.

f) A kiosztott felhasználói jogosultságokat az IBF legalább évente felülvizsgálja.

## 22.2. Kiemelt jogosultságok kezelése

A felhasználói jogosultságok kiadási folyamatánál szigorúbban kell kezelni a kiemelt jogokat biztosító adminisztrátori jogok megadását.

Az elektronikus információs rendszereknél a jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:

a) pontosan meg kell határozni azokat a rendszerelemeket, - pl. operációs rendszereket, adatbázis kezelő rendszert, valamint az alkalmazásokat - és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni;

b) az adminisztrátori jogosultságokat a „feltétlenül szükséges” és az „eseményenkénti” használat elve alapján kell kiadni;

c) az adminisztrátori jogot kizárólag a jegyző engedélyezheti írásban.

Az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá, a részükre biztosított adminisztrátori jogosultság birtokában csak a felhasználó külön engedélyével és jelenlétében, kifejezetten a hiba elhárítása érdekében vagy a felhasználói igény kielégítése érdekében férhetnek hozzá a felhasználók által kezelt információkhoz.

A rendszergazda nem küldhet levelet más felhasználó nevében.

## 22.3. Hozzáférési jogok igénylésének eljárásrendje

Az új hozzáférési jogok igénylését, a jogosultságok módosítását és a jogosultságok visszavonását a jelen fejezetben leírtak szerint kell elvégezni.

### 22.3.1. ASP szakrendszerek hozzáférése

Az ASP szakrendszerekhez történő hozzáférés feltétele, hogy a felhasználó rendelkezzen E-személyivel, melyet a kormányablakokban igényelhet.

ASP szakrendszerekhez történő hozzáférések esetében az új felhasználó létrehozását az önkormányzati ASP adminisztrátornak kell jelezni az igényelt szakrendszer és a szakrendszeri szerepkör megadásával, aki a szükséges hozzáférés birtokában létrehozza a felhasználót az ASP rendszerben, illetve hozzárendeli a szakrendszeri szerepkörökhöz.

Beállítandó jogosultsági elemek:

a) Szakrendszerekhez való hozzáférés:

i) Mely szakrendszerekhez vagy keretrendszeri modulokhoz férhet hozzá a felhasználó.

b) Szerepkörök szakrendszerenként:

i) Összehangolt szerepkör-megnevezések (cél a jó áttekinthetőség)

ii) Ugyanannak a felhasználónak több szerepköre is lehet (ez elsősorban a kisebb önkormányzatok esetén gyakori)

c) Iktatóhelyekhez (iktatási sávokhoz) való hozzáférés:

i) A felhasználó csak a megadott iktatóhelyek iratainak kísérőadatait tekintheti meg.

d) Szervezeti egységekre vonatkozó vezetői jogosultságok:

i) Az iratokba való betekintési jog az előadón kívül az előadó mindenkori vezetőjét is megilleti.

e) Helyettesítési jogosultságok:

i) Szabadságolások kezelése, munkahelyi vezető és titkárnő kapcsolata, közeli munkatársak feladatmegosztása

ii) A módosító műveletek automatikus naplózásakor a helyettesítő kiléte is tárolódik.

Az ASP szakrendszerek esetében az önkormányzati ASP adminisztrátor nyilvántartást vezet jogosultságokról.
A nyilvántartás a következő elemeket tartalmazza:

a) szakrendszer megnevezése;

b) felhasználó neve, beosztása;

c) szerepkör megnevezése (esetleg többlet jogosultságok);

d) jogosultság beállításának dátuma.

A kilépő felhasználókról a személyügyi ügyintézőnek értesítenie kell az önkormányzati ASP adminisztrátort, aki visszavonja a kilépő felhasználó jogosultságait.

A kiosztott jogosultságokat az önkormányzati ASP adminisztrátor évente felülvizsgálja és - az adatgazdákkal egyeztetve - a nem szükséges jogosultságokat visszavonja.

### 22.3.2. Hivatali rendszerek hozzáférése

### 22.3.3. Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését a jelen IBSZ *{5. sz. melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlap kitöltésével kezdeményezi. Hozzáférési jogot az igényelhet, akinek a feladatellátásához az szükséges.

Az űrlapon meg kell jelölni az igényelt jogosultság szintjét, azt az időszakot, amelyre a jogosultságot biztosítani kell, illetve a jogosultságigénylés indoklását.

A kitöltött űrlapot alá kell írattatni a munkahelyi vezetővel, aki igazolja, hogy a feladatellátáshoz szükséges a jogosultság biztosítása.

Az űrlapot ezután meg kell küldeni az adatgazda részére, aki jóváhagyja a jogosultságigénylést.

A jóváhagyott jogosultságigénylési űrlapot ezután el kell küldeni rendszergazda részére, aki intézkedik a jogosultság kiadásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jelen IBSZ *{6. sz. melléklet – Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.

A feldolgozás második lépése: a rendszergazda az igényelt beállításokkal létrehozott felhasználói fiókról telefonon vagy személyesen értesíti az igénylőt, és megadja a belépéshez használatos felhasználói nevet, és az első belépést lehetővé tevő kezdeti jelszót és szükség esetén egyéb fontos adatokat.

A feldolgozás harmadik lépése: a kért feladatok elvégzésének bizonylatolása érdekében a rendszergazda aláírja a kitöltött jelen IBSZ *{5. sz. melléklet – Jogosultságigénylési űrlap}* mellékletét, valamint e-mail-en tájékoztatja az igénylőt és a jóváhagyót a jogosultságok megadásáról és a felhasználói névről.

Az aláírt űrlapok ezek után a rendszergazdánál kerülnek tárolásra visszakereshető formában.

Az IBF az említett adatlapok meglétét és a tényleges jogosultság kiadását bármikor ellenőrizheti, és véleményét írásba foglalhatja, amelyet az Hivatal a jogosultsági rendjének folyamatos javítására használ fel.

### 22.3.4. Hozzáférési jog módosítása

A munkahelyi vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a jelen IBSZ *{5. sz. melléklet – Jogosultságigénylési űrlap}* mellékletét.

Az eljárásrend megegyezik az *{22.3.3 Új hozzáférési jog igénylése}* fejezetben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

### 22.3.5. Hozzáférési jog visszavonása

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a jelen IBSZ (5- számú melléklet - *Jogosultságigénylési űrla)* mellékletében található űrlapon kell kezdeményezni.

Az űrlapot ezután el kell küldeni a rendszergazda részére, aki intézkedik a jogosultság visszavonásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jelen IBSZ
(*6. sz. melléklet - Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.

A feldolgozás második lépése: a rendszergazda visszavonja a jogosultságot.

A feldolgozás harmadik lépése: a rendszergazda aláírja a jelen IBSZ *(5. sz. melléklet – Jogosultságigénylési űrlap)* mellékletében található, kitöltött űrlapot, valamint e-mail-en tájékoztatja a munkahelyi vezetőt a visszavonás tényéről.

### 22.3.6. A felhasználói hozzáférési jogok felülvizsgálata

Ellenőrizni kell, hogy a kiadott hozzáférési jogosultságok szintje alkalmas-e a kívánt célra (biztosítja-e az elvárt logikai védelmet). Ennek érdekében a kiosztott hozzáférési jogokat az IBF legalább évente felülvizsgálja.

## 22.4. Hozzáférés ellenőrzés érvényre juttatása

Az elektronikus információs rendszereknek az IBSZ-szel összhangban érvényre kell juttatnia a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

## 22.5. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatalban nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

## 22.6. Külső elektronikus információs rendszerek használata

A Hivatal belső elektronikus információs rendszereinek hozzáféréséhez csak olyan biztonságos infokommunikációs eszköz használható, amely megfelel a következő követelményeknek:

a) Az eszközökön a felhasználóknak rendszergazdai jog nem adható.

b) Az eszközökön naprakész kártékony kód elleni védelmet kell megvalósítani.

c) Az eszközökön az operációs rendszer és a felhasználói programok naprakészségét biztosítani kell.

d) Az eszközökön bekapcsolt tűzfalat kell alkalmazni.

A felhasználók képzésénél kiemelt figyelmet kell fordítani ezen eszközök biztonságos kezelésére.

A felhasználókat egyedileg kell azonosítani és a hálózati kapcsolatot szabványos kriptográfiai módszerrel titkosítani kell.

## 22.7. Nyilvánosan elérhető tartalom

Az információk közzétételével kapcsolatban a Hivatal a jogszabályokat, a vonatkozó belső szabályzatát és az erkölcsi normákat követi.

# 23. Naplózási eljárásrend

A Hivatal elektronikus információs rendszeriben az alábbi naplózási eljárásrendet kell kialakítani.

Az önkormányzati ASP rendszer szakrendszerei naplózásának a kialakítása a működtető feladata.

## 23.1. Naplózható események

Biztosítani kell, hogy az alkalmazott elektronikus információs rendszerek a következő eseményeket naplózni tudják:

a) a felhasználók adminisztrációs tevékenysége:

- bejelentkezés;
- kijelentkezés;
- jelszómódosítás.

b) az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;

c) a rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;

d) a rendszergazdák tevékenysége a rendszer bármely rétegében;

e) a felhasználói jogosultságok módosítása;

f) rendszer események, esetleges hibák;

g) konfigurációs beállítások módosítása.

h) Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóba kell rögzíteni.

Az elektronikus információs rendszerek naplózása kialakításakor be kell vonni a rendszer adatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyeket az adatgazdák igényelnek.

## 23.2. Naplóbejegyzések tartalma

A naplóbejegyzéseknek a következőket kell tartalmaznia:

a) a rendszerelem azonosítóját,

b) az adatazonosítót (fájl / rekord / mező),

c) az esemény ismertetését / a funkcióazonosítót,

d) a felhasználó azonosítóját,

e) az esemény időpontját,

f) az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

## 23.3. Időbélyegek

Az elektronikus információs rendszereknek a naplóbejegyzésekhez készített időbélyegeket a rendszer belső órái alapján kell elkészítenie.

A Hivatalnak szinkronizálnia kell a rendszer belső rendszer órákat a belső, illetve a külső időszolgáltatóval.

## 23.4. A napló információk védelme

Az elektronikus információs rendszereknek a jelen IBSZ-ben foglaltaknak megfelelően meg kell védenie a napló információkat és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

### 23.5. A naplóbejegyzések megőrzése

A biztonsági események utólagos kivizsgálása érdekében a naplóbejegyzéseket 1 évig meg kell őrizni.

### 23.6. Naplógenerálás

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

a) biztosítják a naplóbejegyzések előállítási lehetőségét a *{23.1 Naplózható események}* pontban meghatározott naplózható eseményekre;

b) lehetővé teszik meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;

c) naplóbejegyzéseket állít elő a *{23.1 Naplózható események}* pontban meghatározottak szerinti eseményekre az *{23.2 Naplóbejegyzések tartalma}* pontban meghatározott tartalommal.

## 24. Rendszer és információ sértetlenségre vonatkozó eljárásrend

Az önkormányzati ASP rendszer szakrendszerei és az azokban kezelt sértetlenségének biztosítása – a hivatali munkaállomások kivételével - a működtető feladata.

A Hivatal elektronikus információs rendszerei, illetve az azokban kezelt adatok sértetlenségére vonatkozóan az alábbi eljárásrendet kell alkalmazni.

### 24.1. Hibajavítás

A rendszerprogramokkal kapcsolatos bármely konfigurálási, hangolási műveletet csak a rendszergazda végezhet. Az alkalmazáson végzendő, annak bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is - a jegyző engedélye szükséges.

A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára.

Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.

A felhasználói adatok és alkalmazások védelme érdekében a szoftverek módosítása (frissítés, verzióváltás) folyamán az alkalmazáshoz és az adatokhoz történő illetéktelen hozzáférést és az illetéktelen próbálkozást meg kell akadályozni. Gondoskodni kell arról, hogy a telepített alkalmazások, fájlok ne károsodjanak, és a követelményeknek megfelelően működjenek.

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.

Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

#### 24.1.1. Microsoft termékek biztonsági frissítéseinek telepítése

A Microsoft termékek biztonsági frissítéseinek a telepítéséről a megjelenésüktől számított 1 héten belül gondoskodni kell. A biztonsági frissítéseket a rendszergazdának előzetesen tesztelni kell.

### 24.1.2. Nem Microsoft termékek biztonsági frissítéseinek telepítése

A nem Microsoft termékek frissítését a gyártói ajánlások figyelembe vételével kell elvégezni. A biztonsági frissítések telepítése a rendszergazda feladata.

## 24.2. Kártékony kódok elleni védelem

A Hivatalnak meg kell őriznie az elektronikus információs rendszerek és az információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek támadásaival szemben.

A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

a) Munkaállomások és kiszolgálók esetében memóriában rezidens kártékony kód elleni megoldásokat kell alkalmazni.

b) Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

c) Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.

d) A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.

e) A kártékony kód elleni alkalmazásnak az email-ek csatolmányát ellenőriznie kell, a futtatható állományok szűrését be kell kapcsolni.

f) A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.

g) A külső forrásból származó a cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

h) A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.

i) A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert szabályozni kell. A rendszergazdának értesítenie kell az IBF-et. A további teendőket az IBF határozza meg.

j) Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani a hivatali hálózatról és így kell megtenni a szükséges vírusirtást vagy a rendszer újratelepítését.

k) A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

l) Vírusirtó szoftver víruskereső funkcióját legalább évente egyszer futtatni szükséges kártékony kódok, szoftverek keresésére.

### 24.2.1. Vírusriadó

A vírusriadót az IBF javaslatára a Jegyző rendelheti el.

Abban az esetben, ha egyértelműen megállapítható, hogy a tapasztalt jelenségeket vírusfertőzés okozza, és a vírus egy-két gépet fertőzött csak meg, akkor vírusriadót nem szükséges elrendelni. A fertőzött gépeket azonnal le kell kapcsolni a hálózatról, meg kell kísérelni a vírusok kiirtását. Ha ez nem sikerül, akkor vírusriadót kell elrendelni.

Feltétlenül vírusriadót kell elrendelni a következő esetek bármelyikénél:

a) ha a szokásosnál sokkal több vírusincidens történt;

b) a vírusfertőzést magas kockázatúnak értékeli a vírusvédelmi szoftver gyártója;

c) ugyanaz a vírus fordul elő egyszerre kettőnél több gépen, különböző állományokban;

d) valamely számítógépen aktivizálódik a vírus romboló rutinja, vagy a vírus valamilyen effektust (videó, hang stb.) produkál annak ellenére, hogy a vírusadatbázis frissített, a víruskereső motor működött;

e) adatátvitel során, egy számítógépen jelentkező szokványostól eltérő működés, átkerül más számítógépekre is;

f) szerver oldali vírusfertőzés esetén.

A vírusriadó idején a vírus mentesítés szakmai felügyeletét az IBF és a rendszergazda közösen látják el.

### 24.2.2. Teendők vírusfertőzés, vírusriadó esetén

Az IBF feladata a vírus fertőzés kivizsgálásának irányítása, a felelősség megállapítása.

A rendszergazda a feladatai:

a) a vírusvédelmi rendszer támogatójának értesítése;

b) a vírus fertőzés következtében szükséges intézkedések koordinálása;

c) a fertőzés tényének és a foganatosított intézkedéseknek a rögzítése;

d) a vírusos számítógép leválasztása a hálózatról;

e) a felhasználók értesítése a vírusról;

f) az e-mail rendszer leállítása, ha mail-ben terjedő vírusról van szó;

g) a hálózaton terjedő vírus esetén a külső kapcsolat megszakítása;

h) a vírus adatait tartalmazó vírus tudásbázis letöltése és teljes vírusellenőrzés végrehajtása;

i) a fertőzöttség lehetőségeinek feltérképezése, gondolva a hálózaton, cserélhető adathordozók által, vagy e-mail-en történő fertőzésekre;

j) a kliensek frissítése;

k) manuális vírus ellenőrzés végrehajtása azokon a munkaállomásokon, amelyek megfertőződhettek;

l) amennyiben az a hivatalon kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;

m) a vírus fertőzés okának kivizsgálása a vírusvédelmi szoftver támogatójával közösen.

## 24.3. Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

Az elektronikus információs rendszerek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

A fenti feladatok végrehajtása a rendszergazda feladata.

A rendszergazdának ismernie kell a Hivatal rendszereszközeinek, elektronikus információs rendszereinek működését és azok figyelmeztető és hibaüzeneteit. A szükséges reagálásokat tartalmazó leírást tudniuk kell alkalmazni.

A rendszergazdának rendszeresen el kell végeznie azokat a tevékenységeket, amelyek alapján meggyőződhet arról, hogy az elektronikus információs rendszer üzemszerűen működik.

Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolni kell, valamint az operációs rendszer beállításait rendszeresen menteni kell.

Az üzemeltetési eljárások megfelelőségét az információbiztonsági felülvizsgálatok alkalmával az IBF felülvizsgálja, a szükséges módosításokat átvezetik, a jegyző pedig jóváhagyja.

### 24.4. A kimeneti információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban a Hivatal Iratkezelési Szabályzatával összhangban a következők az előírások:

a) gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,

b) gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódik,

c) gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,

d) biztosítani kell, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

## 25. Rendszer és kommunikáció védelmi eljárásrend

Az önkormányzati ASP rendszer szakrendszereinek és azok kommunikációjára vonatkozó védelem a működtető feladata.

A Hivatal hatásköre a hivatali határvédelemig terjed.

Az elektronikus információs rendszerek és a kommunikáció védelmére vonatkozóan a következő eljárásrendet kell alkalmazni.

### 25.1. A határok védelme

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférést a következő módon kell ellenőrizni:

a) **Minden tilos, ami kifejezetten nincs megengedve!** Ez azt jelenti, hogy alaphelyzetben mindenforgalmat tiltani kell, majd csak azt megengedni, amelyre valóban szükség van.

b) A belső hálózat irányából az internet irányába kapcsolatot csak azokra a protokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.

c) Kifejezetten tiltani kell a belső hálózat irányából az internet irányába a levelezési (SMTP) kapcsolatokat.

d) Megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;

e) A felhasználókat jelszóval megfelelően hitelesíteni kell;

f) Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

g) A Hivatal belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.

h) Biztosítani kell, hogy a Hivatal elektronikus információs rendszerei alapértelmezés szerint ne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükséges igény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.

i) Kiemelt figyelmet kell fordítani a tűzfal operációs rendszere biztonsági frissítéseinek figyelésére és telepítésére.

j) A tűzfalat úgy kell konfigurálni, hogy az utasítsa el a port letapogatási próbálkozásokat.

A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

A felhasználónak az Internet használata során tilos

a) a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele,

b) az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni,

c) fájlcserélő alkalmazásokat futtatni, illetve nem hivatali munkavégzéshez szükséges letöltéseket végezni,

d) hivatali email címmel nyilvános levelezőlistákra, hírlevelekre feliratkozni.

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

Az IBF köteles ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

A Hivatal központi tűzfalát csak a belső hálózatból vagy a konzolról lehet adminisztrálni. A külső hozzáférés nem engedélyezett.

A fentiek végrehajtása érdekében tűzfal biztonsági politikát kell készíteni, mely tartalmazza a

a) tűzfal kialakítására vonatkozó követelményeket,

b) a tűzfalon engedélyezett portokat, protokollokat és szolgáltatásokat,

c) a tűzfal adminisztrálásával kapcsolatos feladatokat és felelősségi köröket

d) a tűzfal biztonsági politikában foglaltak ellenőrzését.

### 25.1.1. A hálózati szolgáltatások belső használatának szabályozása

A Hivatal elektronikus információs rendszerében a felhasználók csak azokhoz a hálózati szolgáltatásokhoz férhetnek hozzá, amelyek használata a munkavégzésükhöz feltétlenül szükségesek.

A hálózatokkal és a hálózati szolgáltatásokkal kapcsolatosan az alábbiakat kell figyelembe venni:

a) a felhasználókkal meg kell ismertetni azoknak a hálózatoknak és hálózati szolgáltatásoknak a felsorolását, amelyeket igénybe vehetnek;

b) a hálózati kapcsolatokhoz és szolgáltatásokhoz való hozzáférés védelmére szolgáló óvintézkedések és eljárások tartalmazzanak bejelentkezési védelmet vagy más, az alkalmazások jogosításának ellenőrzésére szolgáló védelmet;

A hálózati szolgáltatások használatával kapcsolatos szabályozást összhangban kell tartani a hozzáféréseket meghatározó követelményekkel.

A Hivatal elektronikus információs rendszerében TILOS modemet csatlakoztatni. A Hivatal hálózatában csak olyan Wi-Fi eszköz csatlakoztatható, amely minimum WPA2 (technikai korlátok esetén WPA) titkosítást alkalmaz.

Kockázat elemzéssel kell meghatározni a szükséges védelmet és a megfelelő hitelesítési módszert.

### 25.1.2. ASP hálózati eszközök felügyelete

Az ASP rendszer eléréséhez szükséges eszközöket (ASP router, switch, szünetmentes tápegység) zárt rack szekrényben kell működtetni.

A rack szekrények kulcsait a rendszergazda őrzi.

A menedzselhető hálózati eszközök (switchek) konfigurálásánál a következőket kell elvégezni:

e) az eszközök hálózatba illesztéséről készüljön dokumentáció;

f) az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, jelszó) kerüljenek megváltoztatásra;

g) a hozzáférési azonosítókat zárt borítékban, és biztonságosan zárható helyen kell tárolni;

h) a hálózati eszközöket csak a rendszergazda, valamint szerződésben a hálózati eszközök karbantartására kijelölt fél kezelheti;

i) az eszközök frissítése a legutolsó stabil változatnak megfelelően történjen meg;

j) a menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva;

k) az ASP rendszerhez csatlakozó munkaállomásokat menedzselhető hálózati eszközökre kell kötni;

l) ezeken az eszközökön - az idegen eszközök hálózatba történő csatlakozása elleni védelem megvalósítása érdekében - be kell kapcsolni a port security megoldást.

**A Hivatal belső hálózatához idegen (nem a hivatal tulajdonában lévő) infokommunikációs eszköz nem csatlakoztatható.**

### 25.1.3. A felhasználó hitelesítése külső összeköttetésekhez

A felhasználókat jelszóval hitelesíteni kell és ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

### 25.1.4. Hálózat szegmentálás

A Hivatal hálózatában az infokommunikációs szolgáltatásokat, felhasználókat és elektronikus információs rendszereket szegmentálni kell. A külső felhasználók Internet irányából csak a szükséges elektronikus információs rendszereket érhetik el. A belső hálózatot tűzfal válassza el a többi zónától.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom szűrésére, a lehetőségek korlátozására tűzfalak, tartalomszűrők, illetve meghatározott címekkel a kapcsolat tiltását biztosító megoldások szolgáljanak.

### 25.1.5. A hálózati összeköttetések ellenőrzése

A hálózatok hozzáférését szabályozni, a felhasználók felkapcsolódási lehetőségeit korlátozni kell.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom ellenőrzésére a tűzfalak naplói szolgáljanak.

### 25.1.6. A hálózati üzenettovábbítás ellenőrzése

A hálózati üzenettovábbítás ellenőrzését a tűzfalaknak, illetve kapcsolódó tartalomszűrő és címfordító megoldásoknak, valamint azok naplóinak kell biztosítaniuk.

### 25.1.7. Nyilvános elektronikus információs rendszerek védelme

A Hivatal honlapját web hosting szolgáltató működteti, ezért a vele kötött szerződésben elő kell írni a nyilvánosan elérhető tartalmakkal és rendszerekkel kapcsolatos információbiztonsági követelményeket.

## 25.2. Kriptográfiai védelem

A Hivatalnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére szabványos, a vonatkozó jogszabályokban biztonságosnak minősített kriptográfiai műveleteket kell alkalmaznia.

### 25.2.1. A kriptográfiai óvintézkedések használatának szabályzata

A Hivatal elektronikus információs rendszereiben a kriptográfiai eszközök bevezetése esetén ki kell dolgozni az eszközök biztonságos használatát garantáló szabályozást, melynek a következőket kell tartalmaznia:

a) az eszközök védelmét biztosító előírások;

b) az eszközök felhasználására vonatkozó követelmények;

c) a kulcsok generálására, elosztására, tárolására és megsemmisítésére vonatkozó szabályok;

d) a rejtjelzett adatok visszaállításának szabályai és eljárásai azokra az esetekre, amikor a kulcs megsérült vagy elveszett.

### 25.2.2. Kriptográfiai megoldások alkalmazásának feltételei

A Hivatal elektronikus információs rendszereiben csak olyan kriptográfiai megoldások alkalmazhatók, amelyek:

a) a vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kriptográfiai algoritmusokat és protokollokat használnak;

b) az implementációt külső független szakértő auditálta;

c) alkalmazását az IBF jóváhagyta.

## 25.3. Kriptográfiai kulcs előállítása és kezelése

A kriptográfiai kulcsok védelmének módját a kriptográfiai eszközök biztonságos használatát garantáló szabályozásban kell kidolgozni, az adott elektronikus információs rendszer használatba vételét megelőzően.

A vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kulcsgondozó rendszerek használhatók. A belső előírásokat kriptográfiai utasításban, illetve a megfelelő alkalmazás leírásaiban kell meghatározni.

### 25.4. Mobilkód korlátozása

Az önkormányzati ASP szakrendszerhez kapcsolódó munkaállomások web böngészőiben tiltani kell a következő mobil kódok futtatását:

a) VB Script

b) CGI

c) ActiveX

d) Shockwave

Az alapértelmezett beállításokhoz képest a további szigorításokat kell a web böngészőkben beállítani:

a) Előreugró ablakok - blokkolás

b) Mikrofonok, kamerák hozzáférése - tiltás

c) Automatikus letöltés - rákérdezés

A web böngészők fentieknek megfelelő biztonsági beállításáért a rendszergazda a felelős. A web böngészők helyes beállításait az IBF-nek ellenőriznie kell.

## 26. Rendszer és kommunikáció védelmi eljárásrend

Sásdi Közös Önkormányzati Hivatal Informatikai Biztonsági Szabályzata ..... napjával lép hatályba.

Kelt:

Jegyző

# V. Mellékletek

1. sz. melléklet – Értelmező Rendelkezések

2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

3. sz. melléklet – Biztonsági események jelentése

4. sz. melléklet – Kockázatelemzési és kezelési módszertan

5. sz. melléklet – Jogosultságigénylési űrlap

6. sz. melléklet – Hozzáférések nyilvántartása űrlap

7. sz. melléklet – Felhasználói Informatikai Biztonsági Házirend

8. sz. melléklet – Felhasználói Nyilatkozat

9. sz. melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

10. sz. melléklet – Titoktartási Nyilatkozat

1. sz. melléklet – Értelmező Rendelkezések

Az IBSZ-ben használt, és a gyakorlatban alkalmazott, az információbiztonság tárgykörébe tartozó kifejezések, meghatározások megfelelnek az Ibtv., a Közigazgatási Informatikai Bizottság 25. számú ajánlása Magyar Információbiztonsági Ajánlások és az MSZ ISO/IEC 27001:2006 szabvány és jelen IBSZ 4.1 fejezetében meghatározott jogszabályok által használt kifejezéseknek, és értelmezésük is azonos ezekkel.

(1) Adat: Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

(2) Adatállomány: Valamely elektronikus információs rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

(3) Adatbiztonság: Az adatok jogosulatlan megismerése és kezelése (másolás, módosítás, törlés stb.) elleni szervezési és adminisztratív intézkedések, fizikai védelmi eszközök, műszaki és logikai megoldások összehangolt rendszere.

(4) Adatgazda: Felelős azért, hogy az adott adat teljes életciklusa folyamán az adat megvédéséhez a megfelelő biztonság teljesüljön. Az adatgazda joga és kötelessége, hogy a dolgozók részére meghatározza a munkájuk elvégzéséhez minimálisan szükséges hozzáférés szintjét az adatokhoz.

(5) Alapszintű védelem: Egy elektronikus információs rendszer vagy szervezet számára létrehozott minimális védelem.

(6) Auditálás: Az elektronikus információs rendszer biztonsági mechanizmusainak, a számítógépes tevékenységeknek független szakértők által történő átvizsgálása IT biztonsági szempontból, továbbá a rendszer-ellenőrzések megfelelősségének vizsgálata, a kialakított biztonsági stratégia és a működtetési eljárások megfelelősségének megállapítása céljából.

(7) Azonosítás és hitelesítés: Az adott elektronikus információs rendszer biztonsági mechanizmusok segítségével azonosítja és hitelesíti a hozzá fordulókat, mielőtt valamelyik szolgáltatást biztosítaná. Azonosításra és hitelesítésre három dolog alkalmas: amit az egyed ismer (pl. jelszó, PIN-kód), amit az egyed birtokol (pl. intelligens kártya) és ami az egyed sajátossága (pl. biometrikus jellemzők).

(8) Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

(9) Biztonsági audit napló: A biztonsági auditáláshoz gyűjtött, és esetleg fel is használt adatok.

(10) Biztonsági kockázat: A fenyegetettség mértéke, amely megmutatja, hogy valamely fenyegetés milyen mértékű kárt okozhat, ha kihasználja az elektronikus információs rendszer sebezhetőségét.

(11) Biztonsági mechanizmus: Eljárási módszer, eszköz vagy megoldási elv, ami azt a célt szolgálja, hogy egy vagy több biztonsági követelmény teljesüljön.

(12) Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese

(13) 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;

(14) Elégséges-védelem: A védelem akkor kielégítő erősségű (mértékű), ha a védelemre akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a releváns fenyegetésekből eredő kockázat a szervezet számára még elviselhető szintű vagy annál alacsonyabb.

(15) E-személyi: Olyan hatósági igazolvány, amely a polgár személyazonosságát és a vonatkozó jogszabályban meghatározott adatait közhitelesen igazolja, illetve a polgár törvényben meghatározott esetekben gyakorolhatja vele a külföldre utazás jogát. Az állandó személyazonosító igazolvány emellett – új elemként – alkalmas a polgár elektronikus úton történő közhiteles azonosítására, valamint a vonatkozó jogszabályokban meghatározott kivételekkel – a polgár kérelmére – elektronikus aláírás létrehozására.

(16) Felelősségre vonhatóság: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy az elektronikus információs rendszerrel kapcsolatba kerülő emberek (felhasználók, operátorok, üzemeltetők, külső munkatársak stb.) a biztonsággal kapcsolatos tevékenységükért utólag felelősségre vonhatók.

(17) Fenyegetés: Egy fenyegető tényező lehetősége arra, hogy véletlenül vagy szándékosan kiváltson, kihasználjon egy adott sebezhetőséget. Ez gyakorlatilag egy elektronikus információs rendszeren, vagy tevékenységen belüli bármilyen szoftver, információ, hardver, adminisztratív, fizikai, kommunikációs, vagy személyzeti erőforrás megsértésének vagy elvesztésének a lehetőségét jelenti.

(18) Fenyegetettség elemzés: Az a folyamat, amely felsorolja, jellemzi a vizsgált folyamatok és erőforrások fenyegetettségét (azaz a releváns fenyegetéseket, megvalósíthatóságuk nehézségét)

(19) Fenyegető tényező: Olyan körülmény vagy esemény, amely az adat, illetve információ valamely elektronikus információs rendszerben történő feldolgozásának rendelkezésre állását, sértetlenségét, bizalmasságát vagy hitelességét illetve az elektronikus információs rendszernek és az elektronikus információs rendszer elemeinek működőképességét fenyegetheti. A fenyegető tényezők közé soroljuk nemcsak a személyektől eredő támadásokat, amelyek valamely elektronikus információs rendszer ellen irányulnak, hanem valamennyi szélesebb értelemben vett fenyegetést, mint például véletlen eseményeket, külső tényezők általi behatásokat és olyan körülményeket, amelyek általában magának az informatikának a sajátosságaiból adódnak (pl. tűz, áramkimaradás, adatbeviteli hibák, hibás kezelés, hardver tönkremenetele, kártékony kódok, alkalmazáshibák).

(20) Folytonos védelem: Folytonos a védelem, ha az az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

(21) Helyreállítás: Egy szolgáltatás akkor tekinthető helyreállítottnak, ha a felhasználó újra képes az adott szolgáltatást igénybe venni, azaz az elektronikus információs rendszer és a rendelkezésre álló adatok visszaállítása megtörtént, a szükséges teszteket elvégezték, a felhasználót minderről tájékoztatták.

(22) Hitelesség: A hitelesség az adat olyan biztonsági jellemzője, amely arra vonatkozik, hogy az adat (bizonyíthatóan) egy elvárt forrásból származik. Ehhez szükséges, hogy az informatikai kapcsolatban lévő partnerek kölcsönösen (és egyértelműen) felismerjék egymást, és ez az állapot a kapcsolat teljes ideje alatt fennálljon.

(23) Információs vagyonelemek: Az információs vagyonelemek közé az elektronikus információs rendszer különböző jellegű összetevői tartoznak, például: fizikai infrastruktúra, számítástechnikai eszközök, alkalmazások, adatbázisok és adatállományok, archivált adatok,

rendszerdokumentáció, használói és kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, tartalékolási elrendezések stb.

(24) Információbiztonság: az elektronikus információs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

(25) Kockázat áthárítása: A kockázat kezelés olyan módja, amelynél a kockázatokat (káros hatásokat) megosztjuk egy másik (külső) szervezettel.[3]

(26) Kockázat becslés: Olyan folyamat, amely a releváns fenyegetések szintjét és hatását értékkel jellemzi és megállapítja a fenyegetések szintje, hatásuk, illetve a védelmi igények[4] alapján a kockázatok szintjét.

(27) Kockázat elkerülése: A kockázat kezelés olyan módja, amelynél a felelős vezető úgy dönt, hogy a kockázatos helyzetet eredményező tevékenységet a szervezet nem folytatja tovább.

(28) Kockázat ellenőrzés: Kockázat menedzsment során hozott döntéseket megvalósító tevékenységek tartoznak a kockázat ellenőrzés körébe. Ilyen lehet a kockázatok felülvizsgálata, rendszeres ellenőrzése, illetve a kockázat menedzsment elvárásoknak való megfelelés fenntartása.

(29) Kockázat felmérés: A kockázat elemzést és kockázat kiértékelést átfogó folyamat.

(30) Kockázat felmérési beszámoló: A kockázat felmérés eredmény termékének (dokumentumának) neve, amely a kockázatok ismertetésére szolgál.

(31) Kockázat ismertetés: A döntéshozók és az érintett felek közötti, kockázatokról szóló információ csere vagy tájékoztatás.

(32) Kockázat kezelési terv: A kockázat kezelés eredmény termékének (dokumentumának) neve, amely a kockázat kezelést biztosító intézkedéseket ismerteti[5].

(33) Kockázat kiértékelés: Folyamat, amely során a megbecsült kockázatok összevetésre kerülhetnek a tolerálható szinttel.[6]

(34) Kockázat megtartás: A kockázat kezelés olyan módja, amelynél a lehetséges káros hatásokat (tehát a kockázatokat) a szervezet elfogadja bekövetkezésük esetén.[7]

(35) Kockázat optimalizálása: A kockázat kezelés olyan módja, amelynél a kockázatokat csökkentjük a fenyegetések szintjének és / vagy lehetséges hatásuk csökkentésével, amíg az elfogadható szintre nem csökken.

[3] Törvényi előírások és jogszabályok megtilthatják a kockázat áthárítását. A kockázat áthárítására jó példa a biztosításkötés. Fenyegetett adatok, folyamatok átadása nem kockázat áthárítás (hanem elkerülés).

[4] Olyan súlyozó szempont, amely az érintett felek szemszögéből az érintett adatok és folyamatok érzékenységét, sérülésének közvetlen vagy közvetett kárát fejezi ki.

[5] Tartalmazhatja a kockázat kezelés módját és kiválasztásának indoklását; tevékenységek prioritási rendjét; erőforrás és költségbecslést; mérföldkövek és ütemezés kijelölését; a megvalósítás és ellenőrzés felelőseinek, illetve időpontjainak kijelölését stb..

[6] A kockázatok elviselhetőségének mérlegelését jelenti, melyben segítséget nyújt a jelen dokumentum kockázat kiértékelési fejezetében ismertetett un. tolerancia mátrix.

[7] A kockázatok kiértékelése során felhasznált szempont rendszer ebben segítséget nyújthat.

(36) Kockázatcsökkentés: intézkedések, amelyeket egy kockázattal kapcsolatos valószínűség vagy a negatív következmények (vagy mindkettő) enyhítésére hoztak

(37) Kockázatkezelés: Azoknak a biztonsági kockázatoknak az elfogadható költségen történő minimalizálása vagy megszüntetése, amelyek hatással lehetnek elektronikus információs rendszerekre.

(38) Kockázattal arányos védelem: A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

(39) Kriptográfia: az információ titkos, az illetéktelen hozzáféréssel szemben biztonságos feldolgozásának és továbbításának elmélete és gyakorlata.

(40) Letagadhatatlanság: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy az elektronikus információs rendszerrel kapcsolatos tevékenységek letagadhatatlanok. Ezt a funkciót titkosítási (rejtjelezési) és digitális aláírási technikákra alapozzák.

(41) Maradványkockázat: Az a kockázat, ami a kockázatcsökkentés után megmarad.

(42) Megkerülhetetlenség: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy a védelmet nem lehet kijátszani, azaz az elektronikus információs rendszer egyetlen eleme sem hagyható ki vagy nem kerülhető meg az elektronikus információs rendszer.

(43) Rendelkezésre állás: Az elektronikus információs rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszerelem a szükséges időben és időtartamra használható.

(44) Sértetlenség fenntartása: Biztosítják, hogy az adatot, információt vagy alkalmazás csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak, illetve nem semmisíthetők meg.

(45) Sértetlenség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

(46) Sérülékenység, sebezhetőség: Egy információs vagyon, vagy vagyon csoport gyengesége, hibája vagy hiányossága, amellyel egy fenyegetés vissza tud élni.

(47) Szoftver-vagyontárgyak: A szoftver-vagyontárgyak közé tartoznak: alkalmazási szoftverek, rendszerszoftverek, fejlesztési segédprogramok stb.

(48) Teljes körű védelem: Teljes körű a védelem, ha az az elektronikus információs rendszer összes elemére kiterjed.

(49) Tenant: Az önkormányzati ASP rendszerhez történő csatlakozással bevezetett fogalom: Felhasználók csoportja, akik hozzáférnek a részükre biztosított jogosultságoknak megfelelően az ASP rendszer által nyújtott szolgáltatásokhoz.

(50) Változás-felügyelet: Eljárások, amelyek biztosítják, hogy minden változtatás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változtatás megvalósítás utáni áttekintését is.

(51) Zárt felhasználói kör: Az elektronikus információs rendszer biztonsági mechanizmusai mindenkit kizárnak az elektronikus információs rendszer adott szolgáltatásából, kivéve azokat, akik számára az kifejezetten engedélyezett.

(52) Zárt szolgáltatási kör: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy minden informatikai szolgáltatás tilos az adott elektronikus információs rendszerben, kivéve az, ami kifejezetten engedélyezett.

2. sz. melléklet – A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolása

# A Hivatal elektronikus információs rendszereinek és az azokban kezelt adatok biztonsági osztályba sorolása

| Alkalmazás megnevezése | Alkalmazás leírása | Adatgazda | Rendszerben kezelt adatok | Bizalmasság | Sértetlenség | Rendelkezésre állás | Biztonsági osztály |
|---|---|---|---|---|---|---|---|
| **EKATA** | kataszter nyilvántartó (tárgyi eszköz nyilvántartó) | PÜ irodavezető | vagyonnal kapcsolatos adatok | 1 | 2 | 1 | **2** |
| **E-Iktat** | iktatóprogram | Hatósági irodavezető, Gödrei kirendeltség vezető | ügyiratok | 2 | 2 | 2 | **2** |
| **Helyi Vizuál Regiszter** | népesség nyilvántartás | Hatósági irodavezető, Gödrei kirendeltség vezető | illetékköteles adatok | 2 | 2 | 1 | **2** |
| **WINSZOC** | szociális segélyezési rendszer | Hatósági irodavezető, Gödrei kirendeltség vezető | személyes adatok | 2 | 2 | 1 | **2** |
| ***Önkormányzati adórendszer*** | *Helyi adók nyilvántartása* | Hatósági irodavezető, Gödrei kirendeltség vezető | *helyi adók* *személyes adatok* | 2 | 2 | 2 | **2** |
| ***Gazdálkodási rendszer*** | *pénzügyi-számviteli rendszer* | PÜ irodavezető | *főkönyvi adatok* | 2 | 2 | 2 | **2** |
| ***Keretrendszer*** | | rendszergazda | *Hivatali felhasználók adatai* *A Hivatal szervezeti adatai* *Üzleti naplók* | 2 | 2 | 2 | **2** |

| Alkalmazás megnevezése | Alkalmazás leírása | Adatgazda | Rendszerben kezelt adatok | Bizalmasság | Sértetlenség | Rendelkezésre állás | Biztonsági osztály |
|---|---|---|---|---|---|---|---|
| | | | *Rendszerhasználati statisztikák*<br>*Migrációs adatok*<br>*E-learning tananyagok* | | | | |

3. számú melléklet – Biztonsági események jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és idő pontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:_____év___hó___nap ..... .....

Észlelő aláírása IBF aláírása

---

Az esemény kivizsgálásának leírása:

Tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:

| | |
|---|---|
| ☐ | *Igen* |
| ☐ | *Nem* |

Igényel-e kockázatelemzést az esemény:

| | |
|---|---|
| ☐ | *Igen* |
| ☐ | *Nem* |

Dátum:_____év___hó___nap ..... .....

Információbiztonsági felelős aláírása jegyző aláírása

4. sz. melléklet – Kockázatelemzési és kezelési módszertan

## Kockázatelemzési és kezelési módszertan

A jelen dokumentum célja, hogy a jelen IBSZ *{III.11.1 Kockázatelemzés}* fejezetében foglalt követelmények végrehajtásának módját leírja.

## Vagyonleltár

Az elektronikus információs rendszerekre ható fenyegetettségek különbözőek, attól függően, hogy az elektronikus információs rendszer melyik összetevőjét fenyegetik.

A fenyegetettségek megfelelő azonosítása érdekében a létre kell hozni és értelemszerűen fel kell tölteni a következő vagyonelem csoportokat a Hivatal vagyonelemeivel:

a) Környezeti infrastruktúra
b) Hardver
c) Szoftver
d) Adatok
e) Dokumentumok
f) Humán erőforrások

## Helyzetfelmérés

Az információbiztonsági kockázatelemzés elvégzéséhez fel kell mérni, meg kell ismerni az elektronikus információs rendszereket és azok környezetét, valamint azok jelenlegi információbiztonsági szintjét.

A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

a) Adminisztratív védelmi intézkedések
    i. A Hivatalra vonatkozó jogszabályok, szabályzatok
    ii. Az elektronikus információs rendszerre vonatkozó szabályzatok
    iii. Szerződések, külső felek kezelése
    iv. Alkalmazásfejlesztés, változáskezelés
    v. Jogosultságigénylés
    vi. Biztonsági események kezelése
    vii. Üzemeltetési eljárások
    viii. Szervizelés, eszközcsere, selejtezés
b) Logikai védelmi intézkedések
    i. Mentési megoldások
    ii. Kártékony kód elleni védekezés
    iii. Biztonsági frissítések telepítése
    iv. Hálózat felépítése
    v. Biztonsági rendszerek
    vi. Kriptográfiai megoldások
c) Fizikai biztonság
    i. Beléptetés
    ii. Számítógépterem kialakítása
    iii. Épületben történő közlekedés
    iv. Irodák kialakítása, tiszta asztal, üres képernyő politika.

## Gyenge pontok meghatározása

A helyzetfelmérés alapján megszerzett információk birtokában meg kell határozni az egyes vagyonelemek gyenge pontjait.

## Fenyegetettségek elemzése

Az egyes vagyonelemek gyenge pontjaira bizonyos fenyegetettségek hatnak.

Az informatikai erőforrásokra ható fenyegetettségek vagy fenyegető tényezők (például: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a sérülékeny pontokon keresztül fejtik ki hatásukat, így az ellenük való védekezés legfőbb eleme a sérülékenységek azonosítása és megszüntetése.

Az egyes vagyonelemek gyenge pontjait és fenyegetettségeit *{KIB 25. számú ajánlása: 25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata (IBIV) 1.0 verzió a „gyenge pontok" és a „fenyegetettségek"}* segédletei alapján érdemes azonosítani.

## Sérülékenységek elemzése

A sérülékenység egy bizonyos gyenge pont kihasználása a rá ható fenyegetettség által. Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegetettségek tudják kifejteni a káros hatásukat.

## Kárérték szintek kialakítása, károk rávetítése a vagyonelemekre

A következő kárérték szintek kerültek meghatározásra:

| Kárérték szintje | Kár leírása |
|---|---|
| 1 | 1-es biztonsági osztályba sorolt EIR sérülhet vagy egyéb jelentéktelen kár keletkezik. |
| 2 | Egy adott 2-es biztonsági osztályba sorolt EIR sérül |
| 3 | Több 2-es biztonsági osztályba sorolt EIR sérül |
| 4 | A hivatal valamennyi 2-es biztonsági osztályba sorolt EIR sérül |

A kockázatok megállapításához az elektronikus információs rendszerek vagyonelemeire rá kell vetíteni a kárérték szinteket.

## A bekövetkezési valószínűségek meghatározása

Következő lépésként meg kell becsülni a sérülékenységek bekövetkezési valószínűségét.
A bekövetkezési valószínűséghez a következő értékeket kell használni:

- „4" - bármikor bekövetkezhet
- „3" - gyakori
- „2" - közepes
- „1" - ritka

## Kockázatok meghatározása

Az információbiztonsági kockázatokat a sérülékenység bekövetkezésének a valószínűsége és az okozott kár szorzata fogja megadni.

A kockázatok minősítéséhez a következő kockázati mátrixot kell definiálni:

| Kár<br>Valószínűség | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | NA | NA | A | K |
| 2 | NA | A | K | M |
| 3 | A | K | M | NM |
| 4 | K | M | NM | NM |

A kockázatok jelölése a következő:

- NA - Nagyon alacsony
- A – Alacsony
- K – Közepes
- M – Magas
- Nagyon magas

## Elviselhető kockázatok meghatározása

A Hivatal azt a döntést hozta, hogy minden közepes, illetve közepesnél nagyobb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

| Kár<br>Valószínűség | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | T | T | T | EV |
| 2 | T | T | EV | NT |
| 3 | T | EV | NT | NT |
| 4 | EV | NT | NT | NT |

A táblázatban alkalmazott jelölések értelmezése a következő:

- T – Tolerálható
- NT – Nem tolerálható
- EV – Egyenként vizsgálandó

## Kockázatok kezelése

A nem tolerálható kockázatokat kezelni kell. A Hivatal a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (Kockázat csökkentés);
b) Tudatosan, a következményeket felmérve elfogadja a kockázatot (Kockázat elfogadás);
c) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (Kockázat elkerülés);
d) Áthárítja a kockázatot például biztosítással, vagy megfelelő beszállítói szerződésekkel. (Kockázat áthárítás).

Az egyenként vizsgálandó kockázatokat a „kockázatokkal arányos elvet” figyelembe véve egyenként meg kell vizsgálni, hogy egy adott időtávon a kockázatok kezelésére fordított erőforrás egyenesen arányban van-e az okozott kár mértékével.

## Kockázatcsökkentő intézkedések

A PreDeCo elv alapján a kockázatcsökkentés három szemszögből közelíthető meg:

a) Megelőző jellegű (preventív kontrollok)

   A hibák, gyengeségek, sérülékenységek, illetve ezek kihasználására való lehetőségek kiküszöbölése.

b) Korlátozó vagy javító (korrektív kontrollok)

   Egy veszély hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

c) Észlelő és reagáló (detektív kontrollok)

   A sebezhetőségek támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

## Intézkedési terv

Az el nem viselhető kockázatok kezelésére a Hivatalnak intézkedési tervet kell készítenie az egyes feladatok mellé rendelt felelős, határidő és esetleg költség feltüntetésével.

Az intézkedései tervet az IBF készíti elő a rendszergazda bevonásával és a jegyző hagyja jóvá.

5. sz. melléklet – Jogosultságigénylési űrlap

# Hozzáférési jogok igénylése űrlap

Iktatószám:

Jogosultságigénylő adatai

Igénylő neve: .....
Szervezeti egység: .....
Telefon: .....
Email: .....

Igényelt művelet

Jogosultság kezdete: ..... Jogosultság vége:
.....
Új jogosultság
Jogosultság törlése
Jogosultság módosítása
Jogosultság

Egyéb:.....
.....
.....

Indoklás

A jogosultságigényléshez kapcsolódó feladatellátás megnevezése:
.....
.....

.....
Kelt: ..... igénylő aláírása
Munkahelyi vezetői jóváhagyás
Vezető: .....
Beosztása: ..... .....
Kelt: ..... vezető aláírása
Adatgazdai jóváhagyás
Adatgazda: ..... .....
Kelt ..... adatgazda aláírása
A jogosultságot beállító aláírása
Rendszergazda: ..... .....
Kelt ..... rendszergazda aláírása

6. sz. melléklet – Hozzáférések nyilvántartása űrlap

| Sorszám | Iktatószám | Felhasználó neve | Igényelt jogosultság | Igénylés dátuma | Munkahelyi vezető |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend

# Felhasználói Informatikai Biztonsági Házirend

## 1. ÁLTALÁNOS RÉSZ

### 1.1. A Felhasználói Informatikai Biztonsági Házirend célja

A Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) célja, hogy a Sásdi Közös Önkormányzati Hivatalának (továbbiakban: a Hivatal) elektronikus információs rendszereinek felhasználói részére előírja az információbiztonsági előírások rájuk vonatkozó részét.

A Hivatal elektronikus információs rendszereinek védelme érdekében a Hivatal kidolgozta az Informatikai Biztonsági Szabályzatát.

Az Informatikai Biztonsági Szabályzat (továbbiakban: az IBSZ) tartalmazza valamennyi információbiztonsággal kapcsolatos szabályt, melynek betartásával az érintettek által elvárt szinten tartható a Hivatal elektronikus információs rendszereinek és az azokban kezelt adatok biztonsága.

Az IBSZ számos olyan védelmi intézkedést tartalmaz, amely közvetlenül nem kapcsolódik a Hivatal felhasználóihoz, ezért a jelen FIBH-nak az is célja, hogy egy kivonatot adjon az IBSZ felhasználókra vonatkozó előírásairól, illetve néhány helyen kiegészítse és tovább részletezze az IBSZ-ben foglalt magasabb szinten meghatározott követelményeket.

### 1.2. A FIBH általános követelményei

**A FIBH előírásainak alkalmazása, betartása, illetve betartatása, a jelen IBSZ** *(2.1. Szervezeti-személyi hatály)* **pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A FIBH el nem olvasása nem mentesít a felelősség alól.**

Az információbiztonsági előírások betartása megvédi a Hivatalt és a jelen IBSZ *(2.1. Szervezeti-személyi hatály)* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák a FIBH előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ *(8. sz. melléklet – Felhasználói Nyilatkozat)* mellékletében található nyilatkozat aláírása után lehet használatba venni.

A Hivatal a FIBH-t az IBSZ-szel együtt folyamatosan fejleszti és tökéletesíti.

# 2. BEVEZETÉS

A Hivatal által kezelt információk érzékenysége miatt azok védelme, azaz bizalmas kezelése, sértetlensége, valamint megfelelő szintű rendelkezésre állása kritikus tényező.

A Hivatal elvégezte a jogszabályok által előírt módon az elektronikus információs rendszereinek biztonsági osztályba sorolását, melynek során valamennyi elektronikus információs rendszert besorolta egy 1-5-ig terjedő skálán. Az elektronikus információs rendszer biztonsági osztálya adja meg a védelem elvárt szintjét.

A hivatali ügyviteli folyamatok működése nagymértékben az elektronikus információs rendszereire épül, így ezek kiesése, vagy megsemmisülése esetén a Hivatal egyes funkciói működésképtelenné válhatnak, valamint a Hivatal által kezelt érzékeny információk illetéktelen kezekbe kerülhetnek.

A Hivatal elektronikus információs rendszereinek minden felhasználója személyes felelősséggel tartozik a munkájával kapcsolatban a birtokában lévő, illetve a tudomására jutott információk megfelelő kezeléséért, a biztonsági szabályok betartásáért.

# 3. A FELHASZNÁLÓ JOGAI, KÖTELESSÉGEI ÉS FELELŐSSÉGE

A felhasználóknak az elektronikus információs rendszerek használata során a következők a kötelességeik, jogaik és felelősségeik.

## 3.1. A felhasználó jogai

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára,

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére,

c) információbiztonsági képzésre,

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni,

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

## 3.2. A felhasználó kötelessége

Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.

Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát jeleznie kell munkahelyi vezetőjének.

**Valamennyi alkalmazott köteles azonnal értesíteni a rendszergazdát minden olyan körülményről, ami az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet. A rendszergazda szükség esetén értesíti az információbiztonsági felelőst, aki megteszi a további, szükséges intézkedéseket.**

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

**A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással.**

Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

**A Hivatal infokommunikációs eszközei és elektronikus információs rendszerei elsősorban hivatali munkavégzés céljából használható, azok magáncélú használata tilos!**

A Hivatal a vonatkozó adatvédelmi jogszabályok figyelembevételével jogosult a felhasználó hivatalos elektronikus levelezését és internetforgalmát vizsgálni.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

A Hivatalban az alkalmazottak csak a Hivatal tulajdonát képező informatikai eszközöket és engedélyezett szoftvereket használhatják. Ettől eltérni csak a jegyző engedélyével lehet.

**A rendszergazdát kivéve, tilos a Hivatal számítógépeire szoftvereket telepíteni, és azokat futtatni.**

Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

A nyomtatásra, lapolvasásra, fénymásolásra, faxolásra alkalmas készülékek, multifunkcionális eszközök használatánál ügyelni kell arra, hogy:

a) az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben;

b) illetéktelenek ne férhessenek hozzá, mert belső tárolóikban tárolódott üzenetek visszahívhatók, így illetéktelenek kezébe kerülhetnek;

c) véletlen vagy szándékos átprogramozás során az üzenetek egy nem megfelelő számra kerülhetnek;

d) félretárcsázás vagy hibásan tárolt szám miatt az üzenetek illetéktelen személyhez kerülnek.

## 3.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a szabályok betartásáért;

b) az önkormányzati ASP központ működtetője által közzétett felhasználói biztonsági követelmények betartásáért;

c) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;

e) az elektronikus információs rendszerben végzett műveletekért;

f) a Hivatal infokommunikációs eszközeinek (számítógép, nyomtató, scanner, stb.) szakszerű kezeléséért;

g) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

# 4. AZ INFORMÁCIÓ KEZELÉSÉNEK SZABÁLYAI

## 4.1. Munkaállomások hozzáférés védelme

A felhasználó munkaállomást csak saját nevével és jelszavával belépve használhat. Harmadik fél csak a munkaállomás nevesített felhasználója vezetőjének előzetes írásbeli engedélyével használhat munkaállomást, ebben az esetben is a személyesen hozzárendelt azonosító használatával. Hibaelhárítás vagy támogatás esetén a rendszergazda saját azonosítójával a felhasználó engedélyével a felhasználó munkaállomására beléphet.

**A felhasználónak rendszergazdai jog nem adható!**

## 4.2. A hozzáférés kiosztás folyamata

Az informatikai rendszerekbe belépést lehetővé tevő azonosítót a vezető igényli a felhasználóknak, az IBSZ *{22.3 Hozzáférési jogok igénylésének eljárásrendje}* fejezetében leírt folyamat szerint.

A hálózati belépést lehetővé tevő azonosítót és a jelszót a rendszergazda személyesen adja át az új felhasználónak. Az átadás során a rendszergazda az azonosító használatáról és az egyéb testre szabási lépésekről oktatásban részesíti a felhasználót.

Az önkormányzati ASP szakrendszereihez történő csatlakozás többtényezős hitelesítéssel történik. A felhasználónak rendelkeznie kell E-személyi-vel, valamint kártyaolvasóval.

Az E-személyihez csak a hozzá tartozó PIN kód megadásával lehet hozzáférni. A sikeres azonosítást és hitelesítést követően az ASP rendszer az egyes szakrendszerekhez történő hozzáférés során további azonosító adatokat (felhasználói név, jelszó) kérhet.

## 4.3. Hozzáférés a hálózathoz és az egyes alkalmazói programokhoz

A Hivatal vezetése felügyeli az elektronikus információs rendszerek használatát a visszaélések megakadályozására és jogosult az elektronikus információs rendszer használatát ellenőrizni.

A Hivatal infokommunikációs eszközein működtetett szoftvereket és alkalmazói rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja az alábbiak szerint:

a) A felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz.

b) Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell.

A felhasználói jelszavak képzéséhez az alábbi szabályt kell betartani:

A jelszó legalább nyolc karakter hosszú legyen, és tartalmaznia kell kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

A felhasználói jelszavak alkalmazásakor az alábbi szabályokat kell betartani:

a) a felhasználó a jelszavát köteles titokban tartani,

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben,

c) a felhasználói jelszót TILOS leírni,

d) ha bármilyen jel mutat arra, hogy a jelszó kompromittálódhatott, azonnal meg kell változtatni és értesíteni kell az információbiztonsági felelőst,

e) nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

f) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el.

A felhasználói jelszavak képzésénél az alábbi szempontokat kell betartani:

a) könnyen megjegyezhető, és nehezen kitalálható legyen;

b) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

c) ne legyen a gépnévre vagy a felhasználói névre utaló;

d) ne legyen sorozat.

e) Különös figyelmet kell fordítani az E-személyihez tartozó PIN kód titokban tartására, mivel az E-személyi-vel minősített elektronikus aláírás hozható létre, mely teljes bizonyító erejű magánokiratnak megfelelő joghatással bír.

## 4.4. Hozzáférés védelem mobil infokommunikációs eszköz esetén

A mobilitás miatt sokkal nagyobb veszélynek kitett mobil infokommunikációs eszközök esetében is jelszót kell használni a rendszerbe történő belépéshez. Bár ez a védelem megnehezíti a hozzáférést, a merevlemezt (winchestert) eltávolítva az ott nyíltan tárolt adatok így is megszerezhetők.

A fentiek miatt fokozottan kell törekedni ezen eszközök fizikai védelmére is az elvesztés, illetve ellopás ellen.

Külső munkahelyen történő feladat elvégzése után a keletkezett adatokat a hálózati meghajtóra kell menteni.

A mobil infokommunikációs eszközökről a feleslegessé vált adatokat le kell törölni.

Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

Mobil infokommunikációs eszközök esetén rendszergazda jog felhasználónak nem adható.

## 4.5. Adatmentések, az adathordozók nyilvántartása és tárolása

Az adatokat csak a helyi munkaállomáson kell tárolni, a „központi fájlszerver” megfelelő könyvtárai mentésre és biztonságos tárolásra biztosított.

**A rendszergazda nem vállal felelősséget a helyi gépen tárolt adatokért.**

A rendszergazda a „központi fájlszerver”-en tárolt ügyviteli adatokról meghatározott módon és gyakorisággal mentést készítenek. Ebből adódóan lehetőség van az állományok, adattáblák statikus visszaállítására a mentés időpontjának megfelelő tartalommal. Folyamatok előre-, illetve visszagörgetésére a rendszer nincs felkészítve. Speciális mentési igényekről a rendszergazdát írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

Az adat visszaállítást az adatgazda írásbeli (e-mail) igénye alapján a rendszergazda végzi el.

A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat:

a) utoljára ismert pontos helyét;

b) megnevezését, és a

c) visszaállítandó időpontot.

**A felhasználónak a jogviszonyának megszűnésekor a munkaállomásán és a központi tárhelyen tárolt adatok törlése tilos!**

# 5. FELHASZNÁLÓK SZÁMÍTÓGÉPES KÖRNYEZETE

## 5.1. Számítógépek és a hálózat kezelési előírásai

A felhasználó felelős az infokommunikációs eszközön általa végzett, nyilvánvalóan szakszerűtlen beavatkozásának következményeiért.

**A felhasználó semmilyen infokommunikációs eszközt nem telepíthet a Hivatal elektronikus információs rendszerébe, azok elhelyezését, telepítési módját nem változtathatja meg. Semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat.**

A felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényével a rendszergazdát kell megkeresnie. Az igénylést a munkahelyi vezetővel egyeztetve a jegyző hagyja jóvá.

A rendszergazda bizonyos szoftver elemek telepítését központi szétosztással, automatikusan végzi. Az ilyen távolról történő frissítéskor meg kell várni a frissítés befejeződését, a folyamatot leállítani tilos. El kell fogadni, hogy ez alatt az idő alatt a számítógép valamivel lassabban működik.

**A Hivatal belső hálózatához idegen infokommunikációs eszköz nem csatlakoztatható.**

## 5.2. Internethasználat, web böngészés

**Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!**

Az Internet és az elektronikus levelezés használatának főbb szabályai:

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén a rendszergazda jelentést tesz az információbiztonsági felelősnek, aki eljár az ügyben a jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos Internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi illetve jogellenes tevékenységre.

**Az internetről csak hivatali célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!**

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

### 5.3. E-mail használat

**A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos a hivatali e-mail címüket nem hivatalos minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra stb.)!**

A Hivatal által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata Hivatali munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

Elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására. Egyéb, pl. telefon megerősítést kell alkalmazni.

A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.

Zavaró, félreinformáló levelek, spam-ek küldése, jogtalan megrendelések elindítása tilos, és eljárást vonhat maga után.

**Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ezeket olvasatlanul törölni kell.**

## 6. VÍRUSVÉDELEM

### 6.1. A vírusvédelem alkalmazásának előírásai

A rendszergazda a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert, és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére. Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

Ha a vírus helye nem lokalizálható, a rendszergazda jogosult a hálózat egyes funkcióit, vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

### 6.2. Teendők vírusgyanú esetén

Vírusgyanú esetén a felhasználó köteles azonnal felhívni a rendszergazdát, aki ellátja utasítással, vagy intézkednek a jelzés továbbításáról az információbiztonsági felelős felé.

# 7. AZ INFORMATIKAI ESZKÖZÖK FIZIKAI VÉDELME

## 7.1. Számítógép használatának előírásai

**A munkaállomást és a perifériákat a napi munkavégzés befejezésekor ki kell kapcsolni.** Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (hálózati nyomtatók vagy a modern monitorok többsége stb.). Az infokommunikációs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

## 7.2. „Üres asztal - tiszta képernyő" politika

Az „üres asztal - tiszta képernyő" politika megvalósítása az alábbiakat jelenti:

a) A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);

b) A felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni;

d) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

e) A felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, fax-okban hagyni.

g) Ügyfelet nem szabad felügyelet nélkül az irodában hagyni.

## 7.3. Mobil infokommunikációs eszközök védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;

b) cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek. Gondoljunk erre, és ne hagyjuk őrizetlenül autóban, szállodai szobában stb. (zárjuk el fizikailag, használjuk, ha lehet az értékmegőrzőt, ha nincsenek érzékeny adatok a gépen);

**A mobil infokommunikációs eszközök ellopása esetén:**

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az információbiztonsági felelősnek és a munkahelyi vezetőnek;

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

d) valamennyi rendőrségi jelentést meg kell őrizni és a Hivatal részére át kell adni.

e) Az Önkormányzati ASP rendszerhez hozzáférést biztosító E-személyi kezelésénél különös figyelmet kell fordítani a fentiek alkalmazására.

**Infokommunikációs eszköz eltűnése**

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az információbiztonsági felelősnek és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

# 8. INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK KEZELÉSE

Információbiztonsági eseménynek minősül minden 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, így különösen

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;

b) a rendszer hibás működése vagy túlterhelések (Dos-támadás);

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

j) a nem teljes vagy nem pontos működési adatokból eredő hibák;

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való

visszaélés. Jelentés a biztonsági eseményekről

**A biztonságot érintő eseményekről a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát. A rendszergazda értesíti az információbiztonsági felelőst, aki jogosult az esemény kivizsgálására.**

Amennyiben a biztonsági esemény érinti az önkormányzati ASP rendszer által nyújtott szolgáltatásokat vagy közvetlenül azokban következik be, az eseményt jelenteni kell az önkormányzati ASP rendszer működtetőjének is.

A biztonságot érintő eseményekről szóló jelentések elkészítésére az IBSZ *{3. sz. melléklet – Biztonsági események jelentése}* mellékletét kell használni.

## 8.1. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarra utaló jelek lehetnek, amikor az alkalmazás nem a várt eredményt adja vagy nem a megszokott képernyőképek jelennek meg.

A jelentéshez az IBSZ *{3. sz. melléklet – Biztonsági események jelentése}* mellékletét kell használni. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

a) fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet és

b) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből, illetve kísérletet tenni a hiba elhárítására.

A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Abban az esetben, ha feltételezhető az információbiztonság sérülése, akkor az eseményt a rendszergazdának jelentenie kell az információbiztonsági felelősnek, aki kivizsgálja az eseményt.

8. sz. melléklet – Felhasználói Nyilatkozat

# Nyilatkozat

Alulírott (név: ,.....

beosztás:.....

szervezeti egység: .....),
kijelentem, hogy a Sásdi Közös Önkormányzati Hivatalának Informatikai Biztonsági Szabályzatának/Felhasználói Informatikai Biztonsági Házirendjének tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

....., 201. .....

.....
Aláírás

9. sz. melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

**Információbiztonsági tájékoztatás**

1. Tájékoztatom, hogy a Sásdi Közös Önkormányzati Hivatalnál (továbbiakban: a Hivatal) fennálló köztisztviselői jogviszonya megszűnésének napjától, 201... . .....-től a Hivatal elektronikus információs rendszereihez való hozzáférési jogosultsága megszűnik. Legkésőbb ezen a napon köteles a használatában lévő, a Hivatal elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni.

2. A Hivatalban működő elektronikus információs rendszereket a Hivatal kizárólag hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában a Hivatal fenntartja magának a tulajdonjogot.

3. A Hivatalnak továbbra is hozzáférési lehetősége van az Ön által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

4. Közszolgálati jogviszonyának megszűnését követően nem jogosult a Hivatal elektronikus információs rendszereiben tárolt, közszolgálati jogviszonya folytán készített, illetve megismert adatokat felhasználni, azokat további személyek tudomására hozni, valamint a megismert és használt elektronikus információs rendszerek összetételéről, felépítéséről, működéséről további személyek számára bárminemű információt közölni.

5. A 4-es pontban megfogalmazott jogellenes magatartásnak polgári- és büntetőjogi következményei lehetnek.

6. Jelen tájékoztatás célja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2013. (VII.15.) BM rendelet 3. § (1) bekezdésében foglaltak szerint, az e rendelet 3. számú mellékletében meghatározott követelményeknek a 4. számú melléklet 3.1.6.4.1.3. pontjában meghatározott módon való megvalósítása.

Sásd, 201 ... .

.....
jegyző

A fenti tájékoztatást tudomásul vettem:

Sásd, 201.....

.....
köztisztviselő neve

.....
aláírása

10. sz. melléklet – Titoktartási Nyilatkozat

# TITOKTARTÁSI NYILATKOZAT

Alulírott

Név: .....

Anyja neve: .....

Lakcím: .....

Sz. ig. szám: .....

a ..... munkatársa kijelentem, hogy

a **Sásdi Közös Önkormányzati Hivatal,** mint **Megrendelő**, valamint

..... mint

**Vállalkozó**

között

.....tárgyú,

..... **-én megkötött vállalkozási/megbízási/szállítási szerződés**

keretében elvégzett feladatok során tudomásomra jutott információkat és adatokat bizalmasan kezelem és megtartom. A tudomásomra jutott információkat, adatokat az érdekkörön kívüli személlyel nem közlöm. Ezen felelősségem fennáll azt követően is, ha a

..... -vel való szerződéses jogviszonyom bármely okból megszűnik.

**Sásd, 201 .....**

.....

Nyilatkozó

| | **Tanú 1** | **Tanú 2** |
|---|---|---|
| Aláírás: | ..... | ..... |
| Neve: | ..... | ..... |
| Anyja neve: | ..... | ..... |
| Lakcím: | ..... | ..... |
| Sz. ig. szám: | ..... | ..... |