BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL


Informatikai Biztonsági Szabályzat

Verziószám: 1.0

Dátum: 2023.11.10.

**Tartalomjegyzék**

[1. Az Informatikai Biztonsági Szabályzat 4](#_Toc76645501)

[1.1 A dokumentum célja 4](#_Toc76645502)

[1.2 A dokumentum hatálya 4](#_Toc76645503)

[1.3 A dokumentum minősítése, kötelezettségek 5](#_Toc76645504)

[1.4 Alapfogalmak 5](#_Toc76645505)

[1.5 Kapcsolódó dokumentumok 8](#_Toc76645506)

[1.6 Szerepkörök 9](#_Toc76645507)

[1.7 Tevékenységek 12](#_Toc76645508)

[1.8 Hivatalrendszer belső együttműködése 12](#_Toc76645509)

[2 Hivatal besorolási Nyilatkozata 13](#_Toc76645510)

[3 Rendszerek besorolási nyilatkozata 15](#_Toc76645517)

[4 Adminisztratív Védelmi Intézkedések 16](#_Toc76645518)

[4.1 Szervezeti szintű alapfeladatok 16](#_Toc76645519)

[4.1.1 Informatikai biztonsági szabályzat 16](#_Toc76645520)

[4.1.2 Az elektronikus információs rendszerek biztonságáért felelős személy 17](#_Toc76645521)

[4.1.3 Intézkedési terv és mérföldkövei 17](#_Toc76645522)

[4.1.4 Az elektronikus információs rendszerek nyilvántartása 17](#_Toc76645523)

[4.1.5 Kockázatelemzés 17](#_Toc76645524)

[4.1.6 Biztonsági osztályba, biztonsági szintbe sorolás, Hivatal biztonsági szintje 19](#_Toc76645532)

[4.1.7 Rendszer és szolgáltatás beszerzés 20](#_Toc76645534)

[4.1.8 Üzletmenet- (ügymenet-) folytonosság tervezése 25](#_Toc76645541)

[4.1.9 Az elektronikus információs rendszer mentései 27](#_Toc76645545)

[4.1.10 Biztonsági események kezelése 29](#_Toc76645551)

[4.1.11 Emberi tényezőket figyelembe vevő – személy – biztonság 32](#_Toc76645562)

[4.1.12 Fegyelmi intézkedések 35](#_Toc76645571)

[4.1.13 Viselkedési szabályok az interneten 35](#_Toc76645572)

[4.1.14 Tudatosság és képzés 38](#_Toc76645574)

[5 Fizikai Védelmi Intézkedések 40](#_Toc76645579)

[5.1 Fizikai és környezeti védelem 40](#_Toc76645580)

[6 Logikai Védelmi Intézkedések 46](#_Toc76645596)

[6.1 Tervezés 47](#_Toc76645600)

[6.2 A rendszer fejlesztési életciklusa 48](#_Toc76645604)

[6.3 Konfigurációkezelés 49](#_Toc76645607)

[6.4 Karbantartás 52](#_Toc76645615)

[6.5 Azonosítás és hitelesítés 55](#_Toc76645627)

[6.6 Hozzáférés ellenőrzése 57](#_Toc76645636)

[6.7 Rendszer- és információsértetlenség 60](#_Toc76645648)

[6.8 Naplózás és elszámoltathatóság 63](#_Toc76645656)

[6.9 Rendszer- és kommunikációvédelem 65](#_Toc76645664)

[6.10 Módosítások követése 66](#_Toc76645674)

## Az Informatikai Biztonsági Szabályzat

Az állami és a hivatali szervek elektronikus biztonságáról szóló 2013 évi L Tv. 15. § (1) bekezdés d) pontjában az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII tv. 24 § (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992 évi LXVI 30. § (1) bekezdésében kapott felhatalmazás alapján a(z) Hivatal (továbbiakban: Hivatal) informatikai biztonsági szabályzatát az alábbiakban határozza meg.

1. meghatározza a célokat, a szabályzat tárgyi és személyi (a Hivatal jellegétől függően területi) hatályát,
2. az elektronikus információbiztonsággal kapcsolatos szerepköröket,
3. a szerepkörökhöz rendelt tevékenységeket,
4. a tevékenységekhez kapcsolódó felelősségeket,
5. az információbiztonság hivatalrendszerének belső együttműködését

## A dokumentum célja

Az informatikai biztonsági szabályzat (a továbbiakban IBSZ, vagy Szabályzat) azon alapvető biztonsági normákat és működési kereteket határozza meg, melyek érvényesítésével a Hivatal elfogadható szintre csökkentheti az általa végzett adatkezelés és adatfeldolgozás kockázatait, egyúttal hozzájárulnak a vonatkozó jogszabályokban előírt követelmények teljesítéséhez. A Szabályzat rögzíti a hatálya alá eső adatok, információk informatikai rendszeren történő adatfeldolgozásával szemben támasztott alapvető biztonsági követelményeket valamint a legfontosabb szervezeti feladatokat és felelősségi köröket.

A Szabályzat további célja, hogy iránymutatással szolgáljon a Hivatal informatikai rendszereihez hozzáférési jogosultsággal rendelkező felhasználók számára az informatikai rendszerek helyes használatáról, ismertesse a helyes és biztonságos munkavégzés szabályait, a követendő eljárásokat, továbbá rögzítse a felhasználókkal szemben támasztott elvárásokat és követelményeket.

## A dokumentum hatálya

A Szabályzat tárgyi hatálya kiterjed a Hivatal minden informatikai rendszerére, teljes informatikai környezetére, beleértve minden olyan adathordozót és informatikai eszközt, amin a Hivatal adatait tárolják, feldolgozzák, vagy ügyviteli folyamatait támogatják, illetve az azok létrehozásával, működtetésével, használatával kapcsolatos tevékenységekre.

A Szabályzat személyi hatálya kiterjed valamennyi, a feladatai ellátásához a Hivatal informatikai rendszereit, eszközeit használó, vagy azokhoz hozzáférő köztisztviselőre, ügykezelőre, Munka Törvénykönyve hatálya alá tartozó munkavállalóra, továbbá a Hivatalban megbízási, vagy egyéb jogviszony alapján az informatikai rendszerekhez bármilyen okból hozzáférő személyre (a továbbiakban együttesen felhasználó).

A Szabályzat területi hatálya kiterjed minden olyan épületre, helyiségre, ahol a tárgyi hatály alá eső eszközök megtalálhatók, illetve a tárgyi hatálya alá tartozó tevékenységeket végeznek.

Jelen szabályzatban foglalt elvárások és követelmények a jegyző jóváhagyásával kerültek kialakításra. Azon biztonsági területek esetében, melyeket jelen szabályzat nem fed le, vagy részletesen nem szabályoz, a jegyző határozza meg a követendő eljárásrendet és az alkalmazandó biztonsági elvárásokat, melyek meghatározásához szükség esetén bevonja az elektronikus információs rendszerek biztonságáért felelős személyt.

***E szabályzatban foglaltak be nem tartása, tartatása a Közszolgálati Szabályzatban ill. a PTk-ban leírt szabálysértés és amely a fenti dokumentumokban megfogalmazott következményeket (eljárást) vonja maga után.***

## A dokumentum minősítése, kötelezettségek

Az IBSZ bizalmas minősítésű, korlátozott körben terjeszthető dokumentum. A Szabályzathoz hozzáférési jogosultsággal a Szabályzat személyi hatálya alá tartozók, továbbá a jegyző által feljogosított személyek rendelkezhetnek.

A jegyző felelőssége a szabályzat napra készen tartása, így a jegyző feladata biztosítani, hogy szükség szerint, a Szabályzatot érintő jogszabályi, funkcionális, biztonsági, technológiai vagy egyéb változások esetén a Szabályzat felülvizsgálata megtörténjen.

## Alapfogalmak

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

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

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

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

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

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

7. *auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

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

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

10. *biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

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

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

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

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

15. *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;

16. *életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

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

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

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

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

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

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

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

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

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

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

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

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

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

30. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

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

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

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

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

35. *magyar kibertér:* a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve Magyarország érintett benne;

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

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

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

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

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

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

42. *számítógépes incidenskezelő központ:* az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott hivatalokban tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

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

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

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

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

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

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

## Kapcsolódó dokumentumok

1. 2012. évi I. törvény a munka törvénykönyvéről
2. 2012. évi C. törvény a Büntető Törvénykönyvről
3. 2013. évi V. törvénya Polgári Törvénykönyvről
4. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)
5. 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről (továbbiakban: technológiai vhr)
6. 187/2015. (VII. 13.) Korm. rendelet az az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
7. 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
8. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.)
9. 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról
10. 1995. évi LXVI. törvény a közokiratokról, a közlevéltárakról, és a magánlevéltári anyag védelméről
11. 1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról
12. 1999. évi LXXVI. törvény a szerzői jogról
13. 2015. évi CCXXII. törvény. az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
14. 1993/146. (X. 26.) Korm. rendelet a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról

**Kapcsolódó szabványok, ajánlások**

1. MSZ ISO/IEC 27002:2011: Az információbiztonság irányítási gyakorlatának kézikönyve
2. MSZ ISO/IEC 27001:2014: Az információbiztonság irányítási rendszerei. Követelmények
3. [A KIB 25. számú ajánlása: Magyar Információbiztonsági Ajánlások (MIBA) 1.0 verzió](http://www.ekk.gov.hu/hu/kib/KIB-25-0_MIBA_v1_vegl.pdf)
4. A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások
5. [A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár](http://kovetelmenytar.complex.hu/)

## Szerepkörök

A BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL a részletes hivatali szerepköröket a Szervezeti és Működési Szabályzatban rögzítette.

*BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL (vezető):* az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, stratégiát, politikát határoz meg, felügyeli ezek megvalósulását, forrást biztosít a megvalósításokhoz.

Az informatikai biztonsági feladatok vezetői szintű tervezése, koordinálása, a szabályzatban előírt kontrollok működtetésének biztosítása és azok működésének felügyelete a jegyző feladata. A jegyző felelőssége továbbá az ügyvitel kialakítása során a Hivatalra vonatkozó informatikai biztonsággal kapcsolatos jogszabályi követelmények érvényre juttatása. A jegyző feladata továbbá:

* munkaviszony létesítésével és megszűntetésével kapcsolatos feladatok ellátása
* elektronikus információs rendszer biztonságáért felelős személy kinevezése
* elektronikus információs rendszerek felhasználói jogosultságainak engedélyezése
* fejlesztési igények engedélyezése
* döntés a védelmi intézkedésekről
* gondoskodik arról, hogy az informatikai szolgáltatás nyújtásához igénybe vett harmadik felek szerződéseiben az Informatikai Biztonsági Szabályzat elvárásai érvényre jussanak
* biztosítja a Hivatal munkatársainak rendszeres időközönkénti biztonságtudatossági oktatását, feladata a képzések tematikájának összeállítása, a képzések végrehajtása.
* cselekvési tervben előírt intézkedések előrehaladásának figyelemmel kísérte
* kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal
* biztonsági incidensek kivizsgálása

A vezető a fenti feladatokat delegálhatja, figyelembe véve az összeférhetetlen feladatok egy személyhez történő delegálását.

*Informatikabiztonsági felelős (IBF):* az informatikabiztonsággal kapcsolatban szervezi, és szakmai kompetenciájának megfelelően végrehajtja a Hivatal által meghatározott politikát, célokat, stratégiát. Kapcsolatot tart és felügyeli a feladatok végrehajtásával megbízott személyt, vagy személyeket.

Az elektronikus információs rendszer biztonságáért felelős személyt a jegyző nevezi ki vagy bízza meg. Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló információs rendszer védelméhez kapcsolódó feladat ellátásáért. Ennek során:

* közreműködik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtésében és fenntartásában
* támogatás nyújt az előző pontban meghatározott tevékenységek tervezésében, szervezésében, koordinálásában és ellenőrzésében
* előkészíti a Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot
* felülvizsgálja a Hivatal informatikai biztonsági stratégiáját, szükség esetén aktualizálja azt
* előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe sorolását
* véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal információbiztonsági szabályzatait, szerződéseit
* biztosítja a törvényi megfelelést a Hivatal valamennyi elektronikus információs rendszerének tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésben és kockázatkezelésben, karbantartásban vagy javításban közreműködők esetében
* biztosítja a törvényi megfelelést abban az esetben, ha a Hivatal adatkezelési vagy adatfeldolgozó tevékenységre közreműködőt vesz igénybe
* felülvizsgálja a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását, illetve a Hivatal biztonsági szintbe sorolását
* jegyzői kérésre közreműködik az informatikai biztonsági incidensek kivizsgálásában
* kockázatkezelési javaslatok kidolgozása, megvalósulásuk nyomonkövetése

Az elektronikus információs rendszer biztonságáért felelős személy jogosult a Hivatal tevékenységeihez köthető közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében valamennyi adatot, illetve az elektronikus információs rendszerek biztonságában keletkezetett valamennyi dokumentumot bekérheti.

Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó követelményeket, valamint a feladatköröket a 2013. évi L. törvény szabályozza részletesen.

*Megbízott szervezeti egység vezető (osztályvezető):*

* Együttműködik az információbiztonsági felelőssel az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárások, szabályok, felelősségek, kötelező vagy tiltott tevékenységek, viselkedési szabályok meghatározásában.
* Gondoskodik arról, hogy a felelőssége alá tartozó szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági követelményeket, szabályokat.
* Közreműködik az IBF által tartott előző pontban megjelölt követelmények teljesülésének ellenőrzése során.
* Saját és a felelőssége alá tartozó munkatársak információbiztonsági, informatikai fennakadásáról tett észrevételeit jelenti a rendszergazdának.

*Adatgazda (megbízott szervezeti egység vezető):*

* Meghatározza a hatókörébe tartozó elektronikus információs rendszerekhez, adatokhoz, tevékenységekhez hozzáférők körét.
* Engedélyezi a szükséges jogosultságokat a hatáskörébe tartozó elekrtonikus információs rendszerek, adatok, tevékenységek tekintetében.
* Tájékoztatja a rendszergazdát a felhasználói jogosultság visszavonásáról
* Közreműködik az információbiztonsági kockázatok elemzésében, értékelésében
* Közreműködik az IBF-el az üzeltmenet folytonosság tervezésében

*A rendszergazda* a jegyző iránymutatásának a szerződésben leírtaknak és e szabályzatnak megfelelően végzi feladatait. Szorosan együttműködik az elektronikus információs rendszer biztonságáért felelős személlyel az informatikai biztonsági követelmények kialakításában és végrehajtásában.

*A rendszergazda feladata:*

* A Hivatal informatikai igényeinek (hibák, változások) fogadása, informatikai hibák javítása, informatikai változási igények végrehajtása;
* mentési és naplózási elvárások érvényre juttatása;
* ügyviteli igényeknek megfelelő mentési rend kialakítása és mentési eljárások kidolgozása;
* hatáskörébe tartozó informatikai rendszerek jogosultságadminisztrációs feladatainak ellátása, jogosultság nyilvántartás naprakészen tartása
* a Hivatal elektronikus információs rendszereinek nyilvántartása, beleértve a hardver-, szoftver- és licensznyilvántartás elkészítését
* részvétel az informatikai biztonsági stratégia felülvizsgálatában, megvalósításában
* új elektronikus információs rendszer bevezetése esetén a felhasználók oktatása
* informatikai rendszerek beszerzésében való közreműködés
* a Hivatal elektronikus információs rendszereivel kapcsolatos nyilvántartásainak évenkénti felülvizsgálata.
* Ellátja az Önkormányzat és intézményei számítógépeinek, számítógépes rendszereinek felügyeletét, ezen belül gondoskodik a számítógépek és a kapcsolódó perifériák működőképességéről.
* Közreműködik az intézmények által használt szoftverek telepítésében, gondoskodik működőképességükről, szükség esetén tanácsaival segíti a szoftverek üzemeltetését végző dolgozók munkáját.
* Felügyeli az önkormányzat telekommunikációs rendszereinek (telefon, internet) működését, kapcsolatot tart fenn a telekommunikációs szolgáltatókkal.
* Előkészíti az önkormányzati intézmények informatikai beruházásait, közreműködik a beszerzett számítástechnikai eszközök rendszerbe állításában, esetenként karbantartási feladatokat lát el az eszközök tekintetében

*Beosztottak, alkalmazottak, köztisztviselők:* végrehajtják és betartják az utasításokat, szabályokat. Magatartásukkal segítik a hatékony és biztonságos informatikabiztonság megteremtését. Felhasználó a Hivatal minden munkavállalója, foglalkoztatási formától függetlenül, aki az informatikai rendszereket használja. A felhasználók kötelezettsége a szabályzatban szereplő, illetve a jegyző által előírt védelmi intézkedések körültekintő betartása, alapvető elvárás a felhasználókkal szemben, hogy a napi munkavégzés során az informatikai rendszerek használata során jelen szabályzat szellemiségével összhangban járjanak el.

*A felhasználó:*

* elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználó azonosító kódja (user ID) alapján végeztek
* megakadályozza a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési kódok titkosságát
* betart minden, az informatikai rendszerek megfelelő használatára, tárolására és megsemmisítésére vonatkozó szabályt és az eszközöket a céljuknak megfelelően használja
* a számítástechnikai berendezéseket, programokat előírás szerint használja
* jelenti az észlelt incidenseket, sebezhetőségeket, működésbeli problémákat a rendszergazdának és a jegyzőnek;
* elvárható gondossággal jár el az adatkezelés során, mind az adatbevitel, mind a kimenő adatok elkészítése alkalmával

*ASP adminisztrátor (tenant admin):*

* Az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat, intézmény, nemzetiségi önkormányzat) szintű felhasználó kezelés, azaz:
* Az adott tenant felhasználóinak felvétele és a szakrendszeri szerepkör(ök)höz rendelése, annak adminsztrációja és karbantartása
* Intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása illetve a tanúsítványokat hordozó tokenek csoportos átvétele és felhasználók közötti kiosztása.
* A tenant adminisztrátornak törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében
* Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság- kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen.

*Önkormányzati szakrendszeri adminsztrátor(ok)*

* Feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztációja és karbantartása.

*Honlap tartalom kezelő (Weblap fejlesztő, üzemeltető, tartalom felelős)*

*Weblap fejlesztő*

* Sérülékenységek ellenőrzése és a nyilvánosságra hozott hibák kijavítása, weblap motor, telepített modulok folyamatos ellenőrzése, frissítése

*Üzemeltető*

* Védekezés külső, belső támadás ellen
* Használt szolgáltatások folyamatos frissítése, karbantartása

*Tartalom felelős*

* Jogszabályi követelményeknek megfelelően a tartalom feltöltési és karbantartási feladatok ellátásáért a Hivatal által kijelölt munkatárs felelős
* A Hivatal weboldalán elsősorban hírközlő, információs, tájékoztató jellegű adatokat közöl, a települést mutatja be, aktuális híreket és információkat közöl az állampolgárok számára
* A Weboldalra szánt tartalmat előzetesen jóvá kell hagynia a Hivatal vezetőjének

A Hivatali szerepköröket a Hivatal a munkaköri leírásokban rögzítette.

Harmadik fél szolgáltatásainak igénybe vétele előtt a jegyző feladata, az elektronikus információs rendszer biztonságáért felelős személlyel együttműködve, az informatikai biztonsággal kapcsolatos kockázatok előzetes felmérése, hogy mely kockázatok értékelése alapján fogjuk a későbbiekben kötendő szerződést elkészíteni.

Harmadik félnek tilos megengedni a hozzáférést az információkhoz, információfeldolgozó eszközökhöz, amíg a kellő óvintézkedések (pl. megfelelő titoktartási és bizalmassági nyilatkozat aláírása) foganatosítása nem történt meg és a felek nem állapodtak meg és nem rögzítették a szerződésben.

## Tevékenységek

BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL a törvényben meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

## Hivatalrendszer belső együttműködése

BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL belső együttműködését a Szervezeti és Működési Szabályzatban rögzítette.

## Hivatal besorolási Nyilatkozata

Hivatal nyilatkozatban rögzíti, hogy a 2023.11 hó időszakban a Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával a NEIH által kiadott 41/2015.\_(VII. 15.) BM rendeletnek való megfelelés a [NEIH-SZVI] Szintbe sorolás és védelmi intézkedés űrlapja (v2.10, MS Office) felhasználásával egy kockázatértékelés során végzett a 2013. évi L. tv. 9. §–nak való megfelelés szerinti vizsgálat eredményeként a Hivatal biztonsági szintje:

**3-as (azaz hármas) besorolású**

mert a Hivatal ill.van olyan szervezeti egysége amely elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe továbbá, szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot nem kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója.

A Hivatal a 3-as szint elérésére és fenntartására a következő folyamatokat vezeti be és tartja fenn:

* 1.1.1. a Hivatal az érintett személyi kör részére biztosítja a szervezeti, vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasításokat, belső rendelkezéseket, szabályozásokat, vagy más erre célra szolgáló dokumentumokat ( a tobvábbiakban együtt: szabályzat);
* 1.1.2. az informatikai biztonsági szabályzat részeként egy folyamatos kockázatelemzési eljárást használ, amely tartalmaz beépített ellenőrzési pontokat;
* 1.1.3. az informatikai biztonsági szabályzat egész szervezetre és működési területére vagy meghatározott vagyonelemre, szervezeti egységre vonatkozik;
* 1.1.4. az informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezető hagyja jóvá;
* 1.1.5. az informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;
* 1.1.6. a Hivatal az informatikai biztonsági szabályzat be nem tartását fegyelmi ill. jogi eljárás keretében szankcionálja;
* 2.1.1. az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;
* 2.1.2. mely tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;
* 2.1.3. ezek a folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;
* 2.1.4. ezen folyamatokat a Hivatal olyan szervezeti egységek, vagy személyek felügyelete alá rendeli, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel, vagy szervezeti egységekkel;
* 2.1.5. a folyamatokat és végrehajtásukat a Hivatal úgy dokumentálja, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi köre - megállapítható legyen.
* 3.1.1. az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;
* 3.1.2 a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;
* 3.1.3 a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni, vagy eseti eljárásokra;
* 3.1.4. a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult vezetőnek kell jóváhagynia;
* 3.1.5. a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;
* 3.1.6. a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.

## Rendszerek besorolási nyilatkozata

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (az állami és önkormányzati szervek elektronikus információbiztonságáról) 4. pontja 7. §-a szerint „Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket besorolja egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.” Az önkormányzati ASP rendszerekhez való csatlakozáshoz megvalósítandó informatikai biztonsági követelményeket jelen informatikai biztonsági szabályzat tartalmazza.

Az IT biztonsági műszaki követelmények olyan óvintézkedések (ellenintézkedések), amelyeket az informatikai rendszer és a humán erőforrások valósítanak meg, illetve hajtanak végre a rendszer hardware, software vagy firmware összetevőiben megvalósuló mechanizmusok segítségével. Az informatikai rendszerek biztonságát alapvetően adminisztratív, logikai és fizikai biztonsági intézkedésekkel lehet megteremteni.

**Adminisztratív biztonsági intézkedés:** minden olyan védelmi intézkedés, amely technikai eszközökkel nem, vagy csak részben valósítható meg. Ilyen például egy Informatikai Biztonsági Szabályzat elkészítése vagy egy kockázatelemzés elvégzése.

**Fizikai biztonsági intézkedések:** az adott épület/objektum és az azokban található vagyontárgyak védelmét szolgáló intézkedések, ezek közé tartozik többek között a számítógépterem biztonságának megteremtése (pl.: tűzjelző, riasztó, beléptető rendszer stb.) vagy a munkatársak részére az "üres íróasztal, tiszta képernyő politika" elrendelése.

**Logikai biztonsági intézkedés:** az informatikai rendszerben technikailag beállított vagy kikényszerített védelmi megoldás, ilyen lehet egy megfelelő jelszóházirend beállítása vagy a hálózati tűzfalon csak a szükséges portok, protokollok engedélyezése.

Ahhoz, hogy ezeket a célokat el lehessen érni, bizalmasság, sértetlenség és rendelkezésre állás szempontjából szükséges az egyes rendszerek osztályozása.

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

**Sértetlenség (S)**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek.

**Rendelkezésre állás (R)**: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

A biztonsági osztályba való besorolás célja, hogy kockázatarányos védelmet alakítsunk ki, az elektronikus információs rendszer olyan védelmét, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével, azaz a biztonsági osztályba sorolás a kockázatok alapján az elektronikus információs rendszer védelmi erősségének meghatározása. A Hivatal az elektronikus információs rendszerek biztonsági osztályba sorolásakor a B\S\R követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesíti.

A kockázati érték, nem egy rendszerelem abszolút kockázatos voltát adja meg, hanem a rendszereket állítja sorrendbe, ahol a legnagyobb kockázati értékű rendszer a „leggyengébb láncszeme” és a legnagyobb eséllyel ebben a rendszerben következik be kár, ha nem változtatunk a biztonsági intézkedéseken.

BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL nyilatkozatban rögzíti, hogy a 2023. 11 hó időszakban, Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával egy kockázatértékelés során végzett 2013. évi L. törvénynek és a 41/2015. (VII. 15.) BM rendeletnek való megfelelés a [[NEIH-OVI] Osztályba sorolás és védelmi intézkedések űrlapja (v4.60, MS Office) a 41/2015. (VII. 15.) BM rendelet alapján](http://neih.gov.hu/sites/default/files/dlc/41_2015_BM_VHR_OVI_151015.xltm) felhasználásával végzett vizsgálatának eredményeként a Hivatal rendszereinek biztonsági osztályai a következők:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sorszám:** | **A rendszer megnevezése:** | **Bizalmasság** | **Sértetlenség** | **Rendelkezésre állás** | **Biztonsági osztály** |
|  | ÁNYK | 1 | 1 | 1 | **1** |
|  | ANYAKÖNYV (ASZA) | 2 | 2 | 2 | **2** |
|  | balatonfokajar.hu | 1 | 1 | 1 | **1** |
|  | e-személyi | 2 | 2 | 2 | **2** |
|  | e-szigno | 2 | 2 | 2 | **2** |
|  | KATAWIN | 2 | 2 | 2 | **2** |
|  | ÖNKADÓ | 2 | 2 | 2 | **2** |
|  | Vizuál Regiszter | 2 | 2 | 2 | **2** |
|  | WINSZOC | 2 | 2 | 2 | **2** |

Az elektronikus információs rendszerek besorolása kizárólag azokra az EIR-ekre terjedt ki melyek a Hivatal kezelésében vannak ezért az elektronikus információs rendszerek nyilvántartásában szereplő rendszerek száma eltér a jelen fejezet biztonsági osztályba sorolt rendszerek számától.

A Hivatal az Ibtv. 11. § (3) szerinti a központi adatkezelő és adatfeldolgozó szolgáltató által biztosított nem saját kezelésben működtetett rendszereinek besorolását is saját jogon elvégezte. A Hivatal célja tisztázni a központi adatkezelő és adatfeldolgozó szolgáltatóval, hogy mi a kérdéses rendszerek központi adatkezelő és adatfeldolgozó szolgáltató általi besorolásuk, kétoldalú szerződésben rögzíti, hogy a biztonsági osztályba sorolásból adódó elvárásokból melyik fél mit vállal és milyen kötelezettségek hárulnak rá.

Az informatikai biztonsági szabályzat elsősorban a következő, az érvényes rendeletben meghatározott elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

## Adminisztratív Védelmi Intézkedések

## Szervezeti szintű alapfeladatok

## Informatikai biztonsági szabályzat

A Hivatal megfogalmazta, dokumentálta, valamint kihirdette az informatikai biztonsági szabályzatát. Az informatikai biztonsági szabályzatot a Hivatal, vezető testülete hagyja jóvá.

Az informatikai biztonsági szabályzatát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági szabályzatot újra vizsgálja, szükség szerinti módosítja. A Hivatal az „informatikai biztonsági jelentésben” rögzíti az érintett hivatal elvárt biztonsági szintjét, valamint az érintett hivatal egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

## Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevezett ki (külsős alvállalkozó), aki: ellátja az állami és hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat. A Hivatal vezetője gondoskodik (alvállalkozó esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően.

## Intézkedési terv és mérföldkövei

A Hivatal vezetése intézkedési tervet készít az elektronikus információbiztonsági stratégia megvalósításához az ide vonatkozó törvényben meghatározott határidőkkel, és ebben mérföldköveket határoz meg. Az így elkészített intézkedési tervet legalább évente felülvizsgálja és karbantartja. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosságot állapítanak meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az érintett hivatalra érvényes szint, akkor a Hivatal vezetése a vizsgálatot követő 90 napon belül felülvizsgálatot készít a hiányosság megszüntetése érdekében.

## Az elektronikus információs rendszerek nyilvántartása

A Hivatal az elektronikus információs rendszereiről, minden rendszerre nézve egy elektronikus nyilvántartást vezet, melyet szükség szerint aktualizál. A nyilvántartás tartalmazza:

1. a rendszerek alapfeladatait;
2. a rendszerek által biztosítandó szolgáltatásokat;
3. az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett Hivatal kezelésében vannak);
4. a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
5. a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A Hivatal az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(*Alapkonfiguráció.xlsx*)* kezeli. Felelős: Rendszergazda

## Kockázatelemzés

### Kockázatelemzési eljárásrend

A Hivatal vezetése megfogalmazta, dokumentálta, valamint kihirdette a kockázatelemzési eljárásrendet, mely a kockázatelemzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

### A Hivatal vezetése

1. felelős a kockázatkezelési rendszer(ek) kialakításáért, működtetéséért
2. felelős a kockázatkezelési kritériumok azonosításáért
3. kinevezi a kockázatfelmérésért felelősöket, tevékenységüket felügyeli
4. gondoskodik a kockázatkezelési irányelvek betartásáról
5. biztosítja a kockázatfelméréshez és –kezeléshez a szükséges erőforrásokat
6. dönt a kockázatfelmérés elfogadásáról, kockázatok elfogadásáról, az elfogadható kockázati szintről, a szükséges intézkedésekről, figyelemmel kísérési feladatokról
7. gondoskodik a kockázatkezelés fontosságának tudatosításáról a teljes szervezetben

### A kockázatfelmérésért felelős (Rendszergazda)

A működési és az informatikavédelmi kockázatfelmérésért a jogszabályban meghatározott képzettséggel, tapasztalattal rendelkező belső vagy külső (megbízott) a felelős. (Az IBF kapcsolattartóként felügyeli és ellenőrzi a munkáját.) Felelősségi köre:

1. felelős a kockázat-felmérési módszertan(ok) kialakításáért, jóváhagyatásáért
2. kezdeményezi az éves rendszeres felmérés indítását
3. koordinálja a kockázat-felmérési tevékenységeket
4. javaslatokat tesz kockázatkezelési, javítási intézkedésekre
5. gondoskodik a kockázatkezelési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről
6. rendszeresen tájékoztatja az IBF-en keresztül a Hivatal vezetését a kockázati szint alakulásáról, bekövetkezett kockázati eseményekről
7. felelős a szükséges oktatások megtartásáért, megtartatásáért

### Az IBF

1. a kockázatfelmérésért felelős segítségével azonosítja, felméri, értékeli a területére vonatkozó kockázatokat
2. javaslatot tesz a magas kockázatok kezelésére a saját területére vonatkozóan
3. intézkedik a saját hatáskörükben kezelhető kockázatok csökkentésére, kezelésére
4. felelős a területére eső kockázatok figyelemmel kíséréséért, kezeléséért
5. a kockázatok változása, újak felmerülése esetén aktualizálja a felmérést, tájékoztatja a kockázatfelmérésért felelőst

### A munkatársak

1. felelősek a közzétett, kiadott kockázatkezelési előírások betartásáért
2. feladatuk a nem kezelt, illetve az új vagy változó kockázatok jelzése közvetlen vezetőjüknek és/vagy a kockázatfelmérésért felelősnek.

### Kockázatok elemzése

A Hivatalnak az elektronikus információs rendszerek teljes életciklusában megvalósítja és biztosítja az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszerek és elemeinek sértetlenségét és rendelkezésre állását zárt, teljeskörű, folytonos és kockázatokkal arányos védelmét.

A vonatkozó jogszabályokkal összhangban a kockázatelemzés alapját képezi:

* az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, és az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága;
* a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége

A Hivatal a jogszabályi követelményekhez igazodva a CRAMM alapú kvalitatív kockázatelemzési módszertant használja. Az kockázatelemzéshez használandó kvalitatív skálákat, illetve az alkalmazott kockázati mátrixot az elektronikus információs rendszer biztonságáért felelős személy javaslata alapján jegyző hagyja jóvá. A kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás terjedelmét, nagyságát a szakterületek felelősei határozzák meg a jegyző által jóváhagyott kárértéktáblázat alapján.

A kockázatelemzés során vizsgálandó sérülékenységek és az ezeket kihasználni képes releváns fenyegetések azonosításáért, valamint a káresemények becsült bekövetkezési gyakoriságának meghatározásért és ez alapján a kockázatelemzés elkészítéséért az elektronikus információs rendszer biztonságáért felelős személy felel.

A jegyző felelőssége az elektronikus információs rendszer biztonságáért felelős személlyel együttműködve, gondoskodnia a kockázatelemzés legalább évenként vagy szükség esetén, soron kívül dokumentált módon történő felülvizsgálatáról.

### Kockázatok kezelése

Az elektronikus információs biztonságáért felelős személy feladata, hogy azonosítsa a nem elfogadható kockázatokat okozó sérülékenységeket, javaslatot tegyen az esetleges további kezelendő kockázatot okozó sérülékenységekről, valamint megvizsgálni, hogy a kockázatelemzés eredménye befolyásolhatja-e az elektronikus információs rendszerek biztonsági osztályba sorolását és erről tájékoztatni a jegyzőt.

Az elektronikus információs biztonságáért felelős személy feladata, hogy kockázatkezelési javaslatok kerüljenek kidolgozása. A bevezetendő védelmi intézkedés javaslatokról, illetve a felvállalt kockázatokról a jegyző dönt, egyúttal a feladathoz határidőt és felelőst rendel, valamint biztosítja a feladat végrehajtásához szükséges erőforrások rendelkezésre állását.

A jegyző döntései alapján az elektronikus információs biztonságáért felelős személy által összeállított feladatterv végrehajtásának nyomon követése a jegyző felelősségi körébe tartozik.

Amennyiben a kockázatkezeléssel kapcsolatos vezetői döntések alapján változik az elektronikus információs rendszerek biztonsági osztályba sorolása, a jegyző felelőssége, hogy a Hivatal az új Biztonsági osztályba, biztonsági szintbe sorolás fejezetben leírtak szerint elvégezze a besorolást.

##  Biztonsági osztályba, biztonsági szintbe sorolás, Hivatal biztonsági szintje

Az elektronikus információs rendszerek, valamint az azokban kezelt adatok költséghatékony védelmének biztosítása érdekében a Hivatalnak a vonatkozó jogszabályokban leírtak szerint be soroljuk az elektronikus információs rendszereket egy-egy (1-től 5-ig számozott) biztonsági osztályba a kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kockázata alapján, valamint meghatározzuk a szervezet biztonsági szintjét.

Az elektronikus információs rendszerek biztonsági osztályba sorolását a vonatkozó jogszabályok szerint kockázatelemzés alapján végezzük el, oly módon, hogy a biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást vesszük figyelembe.

A fentiekben leírtaknak megfelelően a Hivatal az elektronikus információs rendszerek biztonsági osztályba sorolását a Kockázatkezelés pontban leírtak szerinti kockázatelemzési, kockázatkezelési feladatok eredményei alapján a NEIH által hivatalosan közzétett segédletek felhasználásával végzi el.

Az elektronikus információs rendszerek biztonságáért felelős személy feladata, hogy a kockázatelemzés, illetve a kockázatkezelési döntések alapján előkészítse az elektronikus információs rendszerek biztonsági osztályba sorolását. Az elektronikus információs rendszerek irányadó biztonsági osztályát az adott információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerint meghatározott kockázata alapján állapítjuk meg.

A biztonsági osztályba, sorolást az elektronikus információs rendszerek biztonságáért felelős személy előterjesztése alapján a jegyző hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.

A jegyző a törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

Az elektronikus információs rendszerek biztonságáért felelős személy feladata, hogy az elektronikus információs rendszerek biztonsági osztályba sorolását és a szervezet biztonsági szintjét jelen szabályzatban rögzítse, valamint a biztonsági osztályba soroláshoz kapcsolódó hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze, aki gondoskodik az adatszolgáltatás teljesítéséről, illetve a módosított szabályzat érvénybe léptetéséről.

Hivatal biztonsági szintbe történő besorolását a vonatkozó jogszabályok szerint a NEIH által hivatalosan közzétett segédletek felhasználásával végzi el. A Hivatal biztonsági szintjének rögzítése és lejelentése a rendszerek biztonsági szintjének lejelentésével, azonos módon végezzük.

### Végrehajtás gyakorisága

A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon vizsgáljuk felül.

A soron kívüli biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni. A soron kívüli felülvizsgálatot akkor is elvégezzük, ha a Hivatal státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

Soron kívüli felülvizsgálatot kezdeményezhet a jegyző, tipikusan a működési környezetben bekövetkezett fenti változások esetén, illetve az elektronikus információs rendszerek biztonságáért felelős személy a kockázatelemzés eredményei alapján.

##  Rendszer és szolgáltatás beszerzés

Az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a Hivatal meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként;

### Általános szabályok

1. Az informatikai eszközök és szoftverek beszerzésénél mindig a beszerzésekre vonatkozó Hivatali és a tv-i szabályok szerint járunk el. A beszerzett számítástechnikai eszközöket és szoftvereket nyilvántartásba vesszük.
2. A rendszergazda egyeztetve az igénylő osztályok vezetőivel értékeli az igényeket, majd a jegyzővel való egyeztetés után, egy fontossági rangsort alkotva, beruházási igényként betervezik a költségvetésbe. Ha nincs az aktuális költségvetésben forrás a beruházásra, akkor nem tervezett beszerzés történik.
3. Az eszközök rendeltetésszerű használatáért a személyi leltár szerint használatra kijelölt személy a felelős.

A Hivatal informatikai rendszerének működtetéséhez és biztonságos üzemeltetéséhez kapcsolódó szolgáltatások (pl.: internet kapcsolat, informatikai eszközök üzemeltetése, karbantartása, stb.) beszerzése során a Jegyző köteles gondoskodni arról, hogy a szolgáltatási szerződés tartalma, illetve a szolgáltatás nyújtása összhangban legyen a Hivatal által elvárt információbiztonsági követelményekkel.

A szervezet informatikai eszközök, rendszereket beszerzésére kizárólag előminősített szállítótól kér ajánlatot. Az előminősítés során meg kell győződni a beszállító-jelölt minőségi, mennyiségi és időbeli teljesítési képességéről. A beszerzési folyamat ajánlatkéréssel kezdődik. Minden beszerzés előtt árajánlatot kell kérni több potenciális szállítótól.

Azokban az esetekben, amikor a Hivatal olyan elektronikus információs rendszert vesz igénybe, amelynek használatához jogszabályi előírásban kerül meghatározásra a szükséges eszközök beszerzésen (pl. ASP) értelemszerűen a követelményeknek megfelelő eszközök beszerzése az elvárt.

Az érintett szervezet az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

* a funkcionális biztonsági követelményeket;
* a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
* a biztonsággal kapcsolatos dokumentációs követelményeket;
* a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
* az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

A szolgáltatók/szállítók felé a releváns információbiztonsági szabályokat kommunikálni szükséges.

A szolgáltatók/szállítók, harmadik személy részére logikai vagy fizikai hozzáférés megadása csak a szállítóval kötött szerződéses megállapodás alapján történhet. A szerződésnek tartalmaznia kell a kockázatokat elfogadható mértékre csökkentő intézkedéseket, szabályokat.

A külső szolgáltatókkal kötött szolgáltatási szerződésekben a Hivatal információbiztonságot érintő elvárásait meg kell határozni.

A szerződésben meg kell határozni, hogy a szolgáltató miként biztosítja a szolgáltatás rendelkezésre állását, a szolgáltatásban érintett és Hivatal tulajdonát képző információ és informatikai eszközök sértetlenségének és bizalmasságának megőrzését. Ha egy szolgáltatás esetén a sértetlenség és a bizalmasság nem biztosítható maradéktalanul az adatbiztonság megőrzésére egyéb eljárásokat kell alkalmazni (pl. titkosítás).

A szerződésben meg kell határozni, hogy a szolgáltató miként képes egy esetleges katasztrófa helyzetben szolgáltatást folytatni. Amennyiben ilyen kitétel nem szerepel a szerződésben a Hivatal feladata a szolgáltatás kiesés esetén alkalmazott eljárás kialakítása, szükség esetén további szolgáltatók és üzemelési helyszínek bevonása a szolgáltatásba.

A Hivatal működése szempontjából kiemelten fontos szolgáltatások vonatkozásában több egyenértékű szolgáltatást kell igénybe venni (kivéve azoknál a szolgáltatóknál, melyek jogszabályi előírás alapján kerültek igénybevételre) vagy legalább tervet kell készíteni a szolgáltatás elvesztése esetén a szolgáltatás újraindítására, átállásra.

Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet.

Az érintett szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat, portokat és szolgáltatásokat.

Az elektronikus információs rendszerre vonatkozó dokumentáció

A Hivatal, ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

* a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
* a biztonsági funkciók hatékony alkalmazását és fenntartását,
* a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;

A Hivatal megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

* a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,
* a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,
* a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;

A Hivatal :

* gondoskodik arról, hogy az információs rendszerre vonatkozó - különösen az adminisztrátori és fejlesztői - dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;
* gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

Az érintett szervezet biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.

A megrendeléseket írásban kell megtenni és a beszerzéshez kapcsolódó feljegyzéseket meg kell őrizni. A beszerzett termékeket, eszközöket a lehetséges mértékig az átvétel során ellenőrizni szükséges.

### A védelem szempontjainak érvényesítése a beszerzés során

Ahhoz, hogy a Hivatal védeni tudja az elektronikus információs rendszert, rendszerelemet vagy a rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen szerződéses követelményként meg kell határozni a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésre az alkalmazadnó védelmi intézkedések funkcionális tulajdonságainak a leírását. Felelős: Rendszergazda, Jegyző

### Hardver beszerzés

A beszerzés és üzembe helyezés előtt a Hivatal Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát elvégezzük. Ezen felül törekszünk az egységes (homogén) eszközpark kialakítására. Felelős: Rendszergazda

### Szoftver beszerzés

A beszerzés és üzembe helyezés előtt a Hivatal Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát elvégezzük. Ingyenes (freeware) alkalmazások esetén ellenőrizzük, hogy üzleti jellegű felhasználásra is szabadon használható-e. A szoftverkörnyezet kialakításánál is törekszünk az egységességre (homogenitásra). Felelős: Rendszergazda

### Kellékanyag beszerzés

Az informatikai üzemeltetéshez szükséges irodatechnikai eszközök megfelelő minőségben és mennyiségben történő készletezése a rendszergazdák feladata. Ezekből a kellékekből mindig akkora készlettel rendelkezünk, mely biztosítja a folyamatos üzletmenetet.

### Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal:

1. szerződéses kötelezettségként követeljük meg, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;
2. szerződésben meghatározzuk az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
3. külső és belső ellenőrzési eszközökkel ellenőrizzük, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

A külső elenktonikus információs rendszer szolgáltatók értékelése és a szolgáltatási szerződések átvizsgálása (ahol az lehetséges) az IBF és a rendszergazda feladata. Az ügymenethez kritikus szállítók felé a releváns információbiztonsági szabályokat kommunikálni szükséges, amelyről a jegyző gondoskodik. A szerződésben meg kell hatátozni, hogy a szolgáltató miként biztosítja a szolgátatás rendelkezésre állását, funkcionális és garanciális biztosnági követelményeket (pl. biztonságkritikus termékek elvárt garanciaszintje), illetve, hogy mik a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények.

A Hivatal eljárásban rögzíti a külső elektronikus információs rendszer felhasználóinak feladatait és kötelezettségeit.

A szolgáltatási szerződésben lehetőség szerinte meg kell határozni, hogy a szolgáltató tevékenységét milyen formában lehet ellenőrizni. Amennyiben erre nincs lehetőség, úgy a szolgáltató munkáját ettől függetlenül ellenőrizni és értékelni kell (pl. a szolgáltatás során tapasztalatok alapján, amelyet a szolgáltató felé kommunikálni szükséges).

A szolgáltatók tevékenységének folyamatos információbiztonsági ellenőrzése az IBF kötelessége. A külső szállítókat, szolgáltatókat, harmadik feleket a rendszergazda nyilvántartja.

A külső szállító, szolgáltató, harmadik fél szolgáltatásában bekövetkező változások információbiztonságot érintő várható hatásait értékelni kell és az ebből eredő kockázatok csökkentése érdekében intézkedni kell.

### Folyamatos ellenőrzés

Az IBF az elektronikus információs rendszerek folyamatos ellenőrzése céljából folyamatba épített ellenőrzési tervet hajt végre. A folyamatos ellenőrzés követelményeit a jelen IBSZ Biztonsági értékelések fejezete tartalmazza.

### Biztonsági elemzés ejárásrend

A Hivatal által használt elektronikus információs rendszerek és működési környezetük védelmi intézkedéseit, a bevezetett intézkedések működőképességét, valamint tervezettnek, az előírt biztonsági követelményeknek megfelelő működését az információbiztonsági felelős felülvizsgálati tevékenysége keretében jogosult ellenőrizni, illetve értékelni:

* új elektronikus információs rendszer bevezetése;
* a kockázatelemzés, illetve helyzetfelmérés;
* a cselekvési, illetve intézkedési tervek végrehajtásának ellenőrzése;
* valamint az IBSZ felülvizsgálata során.

Az értékelés eredményétől függően az információbiztonsági felelős javaslatot tehet a Jegyző számára új védelmi intézkedések bevezetésére, meglévő intézkedések, továbbá a tervek módosítására.

### Biztonsági értékelések

Az információbiztonsági felelős feladata a biztonságértékelés eredményét összefoglaló jelentés elkészítése és megküldése a Jegyző számára.

A biztonsági értékelésről készült jelentés minimálisan az alábbi elemeket kell, hogy tartalmazza:

* az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedések;
* a biztonsági ellenőrzések eredményességét meghatározó eljárásrendek;
* az értékelési környezet, az értékelő csoport, az értékelés célja, az értékelést végzők feladata.

A Jegyző feladata gondoskodni arról, hogy a jelentést a Hivatal által használt elektronikus információs rendszerekkel kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladataik által indokolt mértékben megismerjék.

### A biztonsági teljesítmény mérése

A Hivatal az általa használt elektronikus információs rendszerek biztonsági teljesítményének, illetve az alkalmazott védelmi intézkedések hatékonyságának mérésére az alábbi mutatókat alkalmazza:

|  |  |
| --- | --- |
| **Mérőszám** | **Mérés módja** |
| biztonsági események száma | a biztonsági eseményekről, bejelentésükről készült feljegyzések adott időszakra vonatkozó összesítése |
| az elektronikus információs rendszerek rendelkezésre állása | a rendelkezésre állás elvesztésével járó biztonsági események időtartama, illetve a központilag biztosított szolgáltatások üzemeltetői által rendelkezésre bocsátott mérések alapján |
| az elektronikus információs rendszerekkel kapcsolatba kerülő személyek biztonsági képzésének lefedettsége | a képzésekről készült dokumentumok alapján a részvételi arány meghatározása |
| Előírt dokumentációk elérhetősége | Meg kell vizsgálni, hogy az egyes elektronikus információs rendszerek megfelelően dokumentáltak-e. |
| Mobil eszközök biztonsága | Meg kell bizonyosodni arról, hogy a hivatali adatokat kezelő mobil eszközök közül hány eszközön alkalmaznak megfelelő tároló titkosítást. |

A mérések végrehajtásában az rendszergazda, a Hivatal munkatársai, valamint a Hivatallal szerződéses jogviszonyban álló szervezetek (pl.: szolgáltatást nyújtók) kötelesek közreműködni, ahhoz információkat nyújtani. Az információbiztonsági felelős az adott biztonsági értékelés alkalmával a releváns mérőszámok értékeit figyelembe veszi és felhasználja.

##  Üzletmenet- (ügymenet-) folytonosság tervezése

### Üzletmenet-folytonosságra vonatkozó eljárásrend

Az információk védelmének és a megfelelő rendelkezésre állásának biztosítása érdekében a Hivatal az alábbi módon teljesíti az üzletmenet-folytonossági elvárásokat:

1. biztosítjuk, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezetnél (ne sérüljön az SLA);
2. megfelelő alapot adunk a kockázatok csökkentésére irányuló hatékony intézkedések végrehajtásához és eredményességük nyomon követéséhez;
3. meghatározzuk azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a Hivatal folyamatos működése biztosítva legyen;
4. meghatározzuk azokat az intézkedéseket, feladatokat, melyeket az esetleges folytonosság megszakadásra felkészülésként, illetve bekövetkezésekor a kár enyhítéseként, illetve a helyreállításért kell tenni;
5. biztosítjuk, hogy az üzletmenet-folytonosság és a szolgáltatások rendelkezésre állása személyes felelősséghez köthető legyen;
6. biztosítjuk, hogy a Hivatal közép és hosszú távú stratégiáihoz és céljaihoz illeszkedjen;

### Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A Hivatal vezetése által az elektronikus információs rendszerekhez készíttetett BCP Terv tartalmazza az adott elektronikus rendszer (szolgáltatás) üzletmenet-folytonossági tervét is, amely:

1. összhangban áll az Informatikai Biztonságpolitikával, valamint igazodik a szervezet felépítéséhez és architektúrájához;
2. összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
3. meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
4. az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;
5. tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, személyeket és Hivatali egységeket;
6. gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
7. meghatározza az alapfeladatokat (a biztosítandó szolgáltatásokat és azok elvárt szolgáltatási szintjét [angolul SLA]) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
8. rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
9. jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
10. fenntartja a Hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
11. kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

Az üzletmenet-folytonossági terv elkészítése és karbantartása az információbiztonsági felelős feladata, aki a terv kidolgozásába bevonja a rendszergazdát illetve az érintett területek vezetőit.

A Hivatal működésének folytonosságával kapcsolatos feladatok tervezése, irányítása, koordinálása, a szükséges erőforrások rendelkezésre állásának biztosítása a jegyző feladata. A feladat keretében a jegyző alapvetően biztosítja, hogy informatikai szolgáltatás kiesésével járó rendkívüli esemény esetén

* az informatikai szolgáltatás elfogadható időn belül és elfogadható adatveszteség mellett újraindítható legyen;
* az informatikai szolgáltatás kiesésének idejére azon kritikus fontosságú folyamatoknál, ahol ez indokolt a kieső informatikai szolgáltatás használata nélkül működtethető alternatív folyamat biztosítsa a szükséges minimális szinten a működést;
* a Hivatal működését érintő rendkívüli esemény esetén a Hivatal a szükséges tájékoztatási feladatokat szervezett módon végrehajtsa;
* az informatikai szolgáltatás újraindítását követően az ügyviteli folyamatok a normál működési szintnek megfelelően, a normál ügyviteli rend szerint folytathatóak legyenek.

A fentieket figyelembe véve a vonatkozó kockázatokat szem előtt tartva a Hivatal informatikai rendszereit úgy alakítottuk ki, illetve tartalékoljuk, valamint a külső szolgáltató által nyújtott informatikai szolgáltatásokra olyan rendelkezésre állási követelményeket kötünk ki, hogy azok költséghatékonyan támogassák a Hivatal feladatait, illetve az azok alapján az érintett ügyviteli folyamatokra levezethető rendelkezésre állási követelményeket.

A fenti követelmények érdekében számba vesszük a Hivatal működését támogató informatikai szolgáltatásokat, a szolgáltatások rendelkezésre állását veszélyeztető lehetséges rendkívüli eseményeket és meghatározzuk, hogy milyen preventív, detektív, illetve korrektív intézkedések bevezetésével csökkenthetőek az informatikai szolgáltatások kieséséből származó kockázatok elfogadható szintre.

A meghatározott – informatikai szolgáltatás kiesésével járó – rendkívüli esemény bekövetkezése esetén végrehajtandó alternatív folyamat szükségességének meghatározásakor az érintett ügyviteli folyamatok rendelkezésre állási követelményei mellett figyelembe vesszük a Hivatal által használt informatikai rendszerek rendelkezésre állási képességeit (hogyan és mennyi idő alatt lehet a rendszert újraindítani egy esetleges meghibásodást követően és az újraindítás során mikori adatokat lehet a rendszerbe visszatölteni), illetve a külső féltől igénybe vett informatikai szolgáltatások esetén az azokra vállalt rendelkezésre állási paramétereket.

A fenti szempontok figyelembe vételével a jegyző felelőssége meghatározni a Hivatal által alkalmazott kockázatkezelő intézkedéseket; valamint a bevezetett intézkedések működésének biztosítása és felügyelete (pl. az esetlegesen szükségesnek ítélt folytonossági tervek oktatása, tesztelése, rendszeres felülvizsgálata; az informatikai rendszerekre meghatározott rendelkezésre állási képességeket biztosító intézkedések működtetése).

A külső elektronikus információs rendszerek szolgáltató által a Hivatal felé nyújtott szolgáltatások ügymenet-folytonosságának a biztosítása és tervezése, a szolgáltatás üzemeltetését végző feladata (melyet a szolgáltatási szerződés keretében szükséges meghatározni). A Hivatalnak a saját felhasználói környezetében ügyfelei számára szintén biztosítania kell a szolgáltatás folytonosságát egy esetleges kompromittálódást követően is.

A Hivatalon belül kizárólag a folyamatos működés szempontjából kulcsfontosságú személyek számára szükséges kihírdetni az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet.

A Hivatal az elektronikus információbiztonsággal kapcsolatos üzletmenet-folytonossági terveket külön dokumentumban *(BCP terv)* kezeli.

A tervet éves rendszerességgel, illetve szervezeti változások, vagy tesztelés nem megfelelő eredménye esetén minden esetben felül kell vizsgálni. Változások esetén az érintettek felé történő kommunikáció az IBF felelőssége.

A tervek jogosulatlanok számára nem kommunikálhatóak, védeni kell a jogosulatlan hozzéféréstől.

### Folyamatos működésre felkészítő képzés:

Az Üzletmenet-folytonossági terv végrehajtásához kapcsolódó feladatokat minden, a terv végrehajtásában érintett személlyel dokumentált módon meg kell ismertetni. A szükséges képzési forma kiválasztása, a képzés megszervezése, valamint a tervezett képzés tartalmáról, lebonyolításáról az információbiztonsági felelős tájékoztatása a Jegyző feladata és felelőssége. A képzés szakmai tartalmának megfelelőségét a tájékoztatás alapján az információbiztonsági felelős ellenőrzi, illetve hagyja jóvá.

Minden a tervek végrehajtásában, valamint rendkívüli események észlelése és eszkalálási folyamatában érintett munkatársat oktatni szükséges évente legalább egyszer (belépő munkatársat a munkakezdés előtt kell oktatni)

## Az elektronikus információs rendszer mentései

### Általános követelmények

A Jegyző feladata biztosíttatni a rendszergazda bevonásával a Hivatal működése szempontjából kritikus adatok, szoftverek, konfigurációs beállítások megfelelő tartalékolását. A Hivatal informatikai rendszereinek, illetve az informatikai rendszereken kezelt adatoknak a mentését, megőrzését, tárolását úgy oldja meg hogy a mentések típusa, gyakorisága és példányszáma elfogadható adatvesztési kockázatot eredményezzen, valamint az archiválásra vonatkozó jogszabályi követelményeket teljesíthesse.

A Hivatal olyan mentési megoldásokat alkalmaz, illetve olyan mentési eljárást működtet, ami biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, illetve a tárolt adatok sérülése használhatatlanná válása esetén rendelkezésre álljon olyan mentés, amely segítségével a kiesett informatikai szolgáltatás elfogadható időn belül újraindítható, illetve amelynek visszaállításával az elvesztett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetén, amelyek hosszú távú megőrzését a Hivatal elektronikus formában biztosítjuk, hogy a mentések alkalmasnak az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.

A fentieknek megfelelően a rendszergazdának az alábbi irányelveket javasolt figyelembe vennie:

* az adatok mentése illetve archiválása mellett az adatok visszaállításához szükséges valamennyi egyéb adat és szoftver komponens is visszaállíthatóan mentésre, illetve archiválásra kerüljön, vagy mentésük illetve archivált állományuk létezzen,
* a mentésre, illetve archiválásra alkalmazott adathordozó megválasztása az adathordozó felhasználhatóságának gyártói korlátozásai – pl. adatmegőrzési idő, újraírhatóság száma, tárolási előírások stb. - figyelembe vételével történjen,
* a mentéseket tartalmazó adathordozók kezelése a rajtuk tárolt adatok érzékenységének megfelelően történjen, valamint a forrásrendszerrel azonos szintű biztonságos fizikai hozzáférés védelem mellett kerüljenek megőrzésre,
* a mentett és az archív állományok adatainak a visszatöltéséhez szükséges berendezés mindenkor a rendelkezésre álljon.

Egyes rendszerek a programfrissítésük során egy biztonsági mentést végeznek, hogy a sikertelen frissítés esetén vissza lehessen állítani a korábbi állapotot. Ezeket a funkciókat nem tekintjük a Hivatal időszakos mentési politákája részének.

A rendszerek nyilvántartásának részét képezi, hogy milyen időközönként, milyen módon történik mentés az adott rendszerben.

A rendszerek 466/2017. (XII. 28.) Korm. rendeletnek megfefő adattrezorban való archiválása a Kormányzati Felhő üzemeltetője (a rendszer mindenkori adatkezelője) által történik.

Az archiválási kötelezettségnek a hivatal az önkormányzati ASP rendszer útján tesz eleget.

### Feladatok és felelősségek

A mentések szakszerű elvégzését a rendszergazda, vagy a Hivatallal kötött megállapodásban rögzítettek szerint az adott elektronikus információs rendszer üzemeltetője (az ASP esetében a szolgáltató biztosítja) végzi saját adatmentési és naplózási eljárása körében.

A felhasználó felelőssége, hogy az általa használt eszközön (munkaállomáson, laptopon) tárolt azon adatokról, állományokról, amelyek sérülése, elvesztése jelentősen hátráltatná a napi munkavégzést, illetve amelyek pótlása utólag nem lehetséges, vagy túl nagy terhet jelentene a Hivatalra nézve valamiféle mentés készüljön. Az adott eszköz üzemeltetési feladatainak ellátásáért felelős feladata tájékoztatni a felhasználót, hogy mit kell tennie az állományok mentése érdekében (pl. külső adathordozóra írás, hálózati megosztásra történő másolás stb.).

A jegyző joga a mentési feladatok végrehajtásának ellenőrzése, számon kérése.

A Hivatalnál történő mentést a *„Mentési rend”* eljárás részletezi. Az eljárás elkészítése és naprakészen tartása a rendszergazda feladata. A mentéseknek biztosítaniuk kell bármely információbiztonsági eseményekből következő adatvesztések, vagy adat sérülések esetén az adatok hiánytalan visszaállításának lehetőségét, oly módon, hogy azok bizalmassága mindvégig megmaradjon.

### Az elektronikus információs rendszer helyreállítása és újraindítása

A Hivatal évente legalább egyszer a felülvizsgálat alkalmával gondoskodik az elektronikus információs rendszer(ek) utolsó ismert állapotba történő helyreállításának próbájáról és újraindításáról, hogy folyamatossá tegye az ügymenetet egy összeomlást, kompromittálódást vagy hibát követően. Felelős: Rendszergazda.

A Hivatal az elektronikus információbiztonsággal kapcsolatos helyreállítási szabályokat, valamint az elektronikus információs rendszer helyreállításának, újraindításának menetét az érintett dokumentumban *(BCP terv)* kezeli.

### Infokommunikációs szolgáltatások

A Hivatal - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

### Szolgáltatás-prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor az tartalmazza a szolgáltatás-prioritási rendelkezéseket a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

## Biztonsági események kezelése

Biztonsági eseménynek kell tekinteni a nem kívánt vagy nem várt egyedi eseményt vagy eseménysorozatot, amely az elektronikus információs rendszerben kedvezőtlen változást vagy előzőleg ismeretlen helyzetet idéz elő és amely hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, rednelkezésre állása, funkcionalitása elvész, megsérül.

A Hivatal annak érdekében, hogy a biztonsági események által okozható kár minimális legyen az információbiztonsági incidensek tervezett kezelésére jelen fő fejezetben meghatározott eljárásrendet lépteti életbe.

### A biztonsági események kezelése

Az elektonikus információs rendszerben bekövetkezett eseményeket dokumentálni kell a következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében.

Ennek megfelelően az IBF megfogalmazza, dokumentálja a biztonsági eseményekre vonatkozó eseménykezelési eljárást, amely szabályozza az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és helyreállítást.

A Hivatal nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági események típusát, terjdelemét, az általuk okozott károkat, helyreállítás lehetőségeit és költségeit, a helyreállítás időtartamát.

A folyamat működtetése és fejlesztése, a kapcsolódó szabályrendszer naprakészen tartása (személyi változások, infrastuktúra változások, gyakorlati események tapasztalatai, stb. miatt) valamint azok kommunikálása az IBF feladata. A felülvizsgálatot évente minimum egyszer el kell végezni, illetve változások esetén azonnal.

### A biztonsági események figyelése

A Hivatal nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit. A biztonsági eseményekkel kapcsolatos tevékenységeket az IBF koordinálja.

Az elektronikus információs rendszerek működése során fellépő eseményeket megfelelő részletességgel naplózni kell. A rendszergazdának ezeket a naplóállományokat rendszeresen ellenőriznie kell az ellenőrzés eredményéről rendszeresen és szükség esetén időszakosan feljegyzést kell készíteni.

A biztonsági események folyamatos figyelése és észlelése esetén azok jelentése, valamennyi munkatárs, szerződött fél felelőssége.

### A biztonsági események jelentése

Minden vélt vagy valós információbiztonsági incidenst a felhasználóknak azonnal jelenteniük kell a felettesüknek és/vagy a rendszergazdának, aki jelenti azt az információbiztonsági felelősnek. A felhasználó köteles a tapasztalt jelenséget, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul a rendszergazda rendelkezésére bocsátani (pl. feljegyzés, képernyőkép).

*Példák információbiztonsági eseményekre:*

* Betörés, lopás
* Vírustámadás
* Hálózatbiztonsági incidensek
* A fizikai biztonsági rendelkezések megsértése
* Az elektronikus információs rendszerrel való visszaélés
* Bizalmas információk kiszivárgása, kiszivárgásának gyanúja
* Jogosulatlan hozzáférés elektronikus információs rendszerhez vagy rendszerelemhez
* Emberi mulasztás (dokumentált eljárások megszegése)

A biztonsági események észlelésekor, a biztonsági eseményt meg kell szüntetni, vagy az esemény jellegéből adódóan azt igazolni szükséges. Az igazolást azonnal meg kell kezdeni, amelyért a rendszergazda a felelős az érintett felek bevonásával.

Az információbiztonsági incidensekről, valamint annak életútjáról jegyzőkönyvet kell készíteni, amelyet az IBF készít el, és jelenti a Hivatal vezetője felé.

Az IBF jelenti azokat a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervnek, amelyek hálózatbiztonsági incidensből adódnak.

Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni (dokumentálás, eljárások, ellenőrzés, utóvizsgálat stb.) azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP központ és a Kormányzati Eseménykezelő Központ felé is. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adat), elemeket, amelyet harmadik fél nem ismerhet meg. A biztonsági esemény bejelentése során az IBF-nek csatolnia kell a biztonsági eseménnyel kapcsolatos valamennyi információt, az eseményben érintettek beazonosításához szükséges műszaki, technikai adatokat, a biztonsági esemény következményeinek elhárítása érdekében tett intézkedések leírását.

Az ASP hibabejelentő rendszeren keresztül az ASP központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerini lépéseket megteszi.

Ha az önkormányzat ASP-t üzemeltetői, működtetői oldalon éri biztonsági incidens, az ASP Központnak kötelessége értesítést elhelyeznie a Tájékoztatási Portál nyilvánosság elöl elzárt felületén, megjelenítve a lehetséges elhárítási határidőt, illetve a keretrendszer elérhetősége esetén, a keretrendszer felületén is megjeleníteni ezeket az információkat. Ebben az esetben az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.

Amennyiben a biztonsági esemény igazoltan a szabályok megsértéséből adódik, úgy a jegyzőnek le kell folytatnia a szükséges fegyelmi eljárást a Hivatal fegyelmi eljárásra vonatkozó előírásai alapján.

### Biztonsági események kategorizálása

A Hivatal az elektronikus információs rendszereit érintő biztonsági eseményeket két kategóriába sorolja:

* enyhe biztonsági esemény
* súlyos biztonsági esemény

Enyhe biztonsági esemény

A Hivatalban a következők számítanak enyhébb fokozatú biztonsági eseménynek:

* nem kritikus elektronikus információs rendszer vagy adat bizalmassága sértetlensége vagy rendelkezésre állása sérül,
* az ügymenetet jelentősen nem befolyásoló elektronikus információs rendszer rendelkezésre állása sérül,
* a lehetséges társadalmi-politikai hatás szervezeten belül kezelhető.

Súlyos biztonsági esemény:

A Hivatalban a következők számítanak súlyos biztonsági eseménynek:

* egynél több vagy a Hivatal összes elektronikus információs rendszerét érintő biztonsági esemény,
* teljes hálózati infrastruktúrát veszélyeztető esemény,
* személyes adatok illetéktelen kézbe kerülése feltételezhető,
* jogszabály által védett adatok illetéktelen kézbe kerülése feltételezhető,
* személyes adatok, különleges személyes adatok nagy mennyiségben sérülhetnek,
* a bekövetkezett kár mértéke alapján a lehetséges társadalmi-politikai hatás jelentős.

### Segítségnyújtás a biztonsági események kezeléséhez

A felhasználók felé az információbiztonsági események kezeléséhez kapcsolódó információk és irányelvek megadása, tanácsadás és támogatás a feladat- illetve felelősségi körének megfelelően a rendszergazda, illetve az információbiztonsági felelős végzi. A támogatást a felhasználók szükség szerint igényelhetik. A biztonsági események figyeléséről, észleléséről és jelentéséről a felhasználókat oktatni kell.

### Biztonsági eseménykezelési terv

Az IBF megfogalmazza és dokumentálja a biztonsági eseménykezelési tervet. Évente legalább egyszer tervezetten felülvizsgálja, illetve frissíti, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat. Gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Az információbiztonsági események, incidensek kezelési folyamatához kapcsolódóan meg kell határozni és folyamatosan pontosítani kell a biztonsági események kiértékelésének, kategorizálásának (pl. súlyosság) kritériumrendszerét.

Tervezni kell azokat az erőforrásokat és vezetői támogatást, melyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

Az adott esemény biztonsági eseménnyé minősítését kérdéses esetben, illetve annak kiértékelése során az információbiztonsági felelős támogatja, illetve végzi el az eset összes körülményéről rendelkezésre álló információk alapján.

A biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez esetlegesen szükséges további információk (pl.: log fájlok) begyűjtésében a rendszergazda köteles közreműködni.

A biztonsági eseménykezelés a következő folyamatokra terjed ki:

1. Észlelés, jelentés
2. Vizsgálat
	1. Incidensek okának azonosítása, elemzése, kivizsgálása
	2. Bizonyítékok begyűjtése
	3. Incidens behatárolása
	4. A vizsgálat során meg kell állapítani, hogy:
* Milyen események történtek?
* Az események milyen és mekkora kárt okoztak, illetve okozhattak?
* Milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez?
* Mik voltak az események kiváltó okai, előzményei?

Felelős: IBF, rendszergazda, érdekelt munkatársak, kijelölt szakértők

1. Elszigetelés (az esemény jellegéből adódóan)
2. Megszüntetés
	1. A szükséges intézkedések meghatározása
	2. Az incidensekre hozott döntéseket, egyéb feljegyzéseket meg kell őrizni, annak érdekében, hogy ha egy incidens következtében bármilyen peres (polgári vagy büntető) eljárásra kerülne sor, megfelelő bizonyítékként lehessen bemutatni.

Felelős: IBF, rendszergazda, érdekelt munkatársak, kijelölt szakértők

1. Helyreállítás

Helyreállítási felelősök kijelölése:

* 1. Az Üzletmenet-folytonosságot érintő események esetén (az esemény jellegéből adódóan) az Üzletmenet-folytonossági tervben rögzített módon kell eljárni.
	2. A helyreállítási tevékenység ellenőrzése

Felelős: IBF, rendszergazda, érdekelt munkatársak, kijelölt szakértők

A biztonsági esemény jellegétől és várható hatásaitól függően a bekövetkezett vagy okozható kár, kockázat mérséklése, illetve a fenyegetettség vagy veszélyhelyzet elhárítása, megszüntetése érdekében az információbiztonsági felelős által javasolt és szükséges, illetve a Jegyző által meghatározott intézkedések végrehajtásában minden érintett köteles együttműködni.

A biztonsági esemény kezelésének lezárását követően szükség esetén új megelőző védelmi intézkedések bevezetésével kell a hasonló incidensek jövőbeni előfordulásának kockázatát csökkenteni. A biztonsági eseményről rendelkezésre álló információk vizsgálata alapján az információbiztonsági felelős jogosult az indokolt új illetve meglévő védelmi intézkedések módosítására vonatkozó javaslat elkészítése és a Jegyző számára történő megküldése.

### Képzés a biztonsági események kezelésére

Az információbiztonsági incidensekkel kapcsolatos képzések, valamennyi munkatárs felé belépéskor az alap információbiztonsági oktatás részeként megtörténik. Ezen felül évente legalább egyszer, vagy súlyos információbiztonsági események után ismétlődő képzés történik a tudatosság fenntartása, illetve fejlesztése érdekében. A képzéseket az IBF tartja.

## Emberi tényezőket figyelembe vevő – személy – biztonság

### Személybiztonsági eljárásrend

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki a Hivatal elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a Hivatal tagja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

### Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal:

* minden érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot biztonsági szempontból besorol;
* felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat;
* rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

A szükséges képzettségi szinteket, gyakorlati elvárásokat a munkaköri leírásokban, szerződésekben szükséges meghatározni.

### A személyek ellenőrzése

A Hivatal:

* az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy az adott szervezeti munkakörnek vagy a szervezethez kapcsolódó feladat biztonsági szempontból történő besorolásnak megfelelő feltételekkel rendelkezik-e;
* a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat betöltő vagy feladatokat ellátó személyek tekintetében kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést;
* folyamatosan ellenőrzi e pont szerinti feltételek fennállását.

### Eljárás jogviszony megszűnése napján

A jogviszony megszűnésekor az alkalmazottnak, a szerződőknek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz valamint elektronikus informáicós rendszerekhez való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük illetve megállapodásuk lejár. A jogosultságok visszavonása a rendszergazda/adatgazda feladata.

A Hivatal erre jogosult képviselője (rendszergazda):

1. megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;
2. tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;
3. visszaveszi az érintett hivatal elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
4. megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és a Hivatali információkhoz;
5. az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
6. a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
7. a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartására megelőző intézkedéseket tesz.

### A hozzáférési jogok visszavonása

A felhasználó informatikai rendszerekhez való hozzáférési jogát visszavonja az arra jogosult személy a felhasználó jogviszonyának megszűnésekor, illetve módosítja a felhasználó feladatainak változása esetén. A jegyző felelőssége, hogy az egyes felhasználók jogviszonyának megszűnése esetén a Hivatal érintett munkatársait értesítse.

Általánosságban elmondható, hogy a jegyző felelőssége, hogy a felhasználók csak a feladatkörük ellátásához minimálisan szükséges jogosultságokkal rendelkezzenek az informatikai rendszereken. Ennek megfelelően a jegyző felelőssége, hogy:

* a Hivatal informatikai rendszerét üzemeltető megbízott értesüljön a jogosultságok megváltoztatásának szükségességéről
* a jogviszony megszűnésekor az érintett felhasználó hozzáférési jogosultsága visszavonásra kerüljön minden olyan informatikai rendszeren, ahol a felhasználó a jogviszony keretében végzendő feladatai miatt kapott hozzáférést;
* a felhasználó feladatkörének változása esetén az új feladatokhoz már nem szükséges jogosultságok visszavonásra kerüljenek;
* tartós távollét esetén a nem használt hozzáférések felfüggesztésre, illetve tiltásra kerüljenek.

### A vagyontárgyak visszaszolgáltatása

Minden munkatárs köteles a részére átadott vagyontárgyat visszaszolgáltatni a jogviszony megszűnése előtt.

A kilépő munkatárs munkakörét a jegyző által előírt rendben köteles átadni és a munkáltatóval elszámolni. A munkakör-átadás és az elszámolás feltételeit a Hivatal köteles biztosítani.

A jegyző meggyőződik arról, hogy a munkatárs, szerződött parner, harmadik fél minden munkával kapcsolatos adatot és információt, valamint munkájához használt eszközt (laptop, mobiltelefon, stb.) átadott, valamint a jogosultságai és hozzáférései visszavonásra kerültek.

### A munkakör változásának biztonsági kérdései

Áthelyezés esetén a jegyző a jogosultságot kiadóval együttműködve gondoskodik a munkavállaló meglévő jogosultságainak visszavonásáról, majd az új munkakörnek megfelelő új jogosultságok igényléséről. Az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket

### A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Hivatal más, külső szervezettel történő szerződés létesítésekor megköveteli, hogy a partner szervezet rendelkezzen olyan, belső biztonsági szabályozással, amelyben meghatározza a biztonsági szerep- és feladatköröket, felelősségi köröket valamint azonosítja az ilyen feladatkörbe kinevezett vagy azzal megbízott személyeket, rögzíti a velük szembe támasztott elvárásokat.

A partnernek a Hivatalt haladéktalanul tájékoztatnia kell arról, ha változik a saját információbiztonsági felelősének személye, a biztonsági eseményeket kommunikálni jogosult kapcsolattartó személye és/vagy az elérhetőségének módja, illetve ha a Hivatal rendszeréhez bármilyen hitelesítési eszközzel vagy kiemelt jogosultsággal hozzáférő munkatársának jogviszonya megszűnik, vagy munkaköre módosul.

Hitelesítési eszközt vagy a kiemelt jogosultságot a partner nem ruházhat át másik félnek, munkatársank.

A jegyző gondoskodik arról, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

## Fegyelmi intézkedések

Az informatikai rendszerek biztonságának gondatlan veszélyeztetése, az informatikai biztonsági szabályok megsértése, illetve a felhasználó súlyos mulasztása esetén a jegyző felelőssége a szükséges fegyelmi eljárás lefolytatása. A jegyző a fegyelmi eljárás megindításáról köteles írásban értesíteni az érintettet és a vizsgálat végrehajtására vizsgálóbiztost jelöl ki. Az IBSZ hatálya alá tartozó szabályok megszegése esetén a fegyelmi eljárás vizsgálóbiztosa a jegyző. A vizsgálatba a jegyző bevonhatja a rendszergazdát, az elektronikus információs rendszer biztonságáért felelős személyt és más külső szakértőket.

A fegyelmi eljárást a 31/2012. (III.7.) Kormányrendelet rendelkezéseinek megfelelően folytatjuk le.

A fegyelmi vizsgálatról vizsgálati jegyzőkönyvet készítünk, valamint a vizsgálat eredményéről írásban tájékoztatjuk a jegyzőt.

A jelentésnek tartalmazza:

* a biztonságsértés időpontját,
* a biztonságsértést elkövető nevét és beosztását,
* a tevékenység által közvetlenül okozott kárt,
* a tevékenységgel közvetve okozható kár becsült mértékét,
* a felelősségre vonás javasolt módját.

Amennyiben az információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, a jegyző felelőssége érvényesíteni a vonatkozó szerződésben meghatározott és alkalmazható jogi és vagyoni következményeket, továbbá az egyéb jogi lépések lehetőségének vizsgálata és szükség esetén azok alkalmazása.

Ha az IBSZ megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor az elkövetőt írásban figyelmezteti a Hivatal. A figyelmeztetés utáni ismételt elkövetést szándékosnak tekintjük. Különösen súlyos esetben, illetve szándékosság esetén a rendszergazdák a használati jogot megvonhatják és az IBSZ megsértője a teljes információs rendszerből kitiltható. Ha szükséges, az intézmény fegyelmi eljárást, polgári jogi pert is indít. Amennyiben az elkövetett vétség a Büntető Törvénykönyv szerint bűncselekménynek minősül, a Hivatal vezetője köteles a szabályszegővel szemben feljelentést tenni, és a rendelkezésre álló bizonyítékokat az eljáró hatóságok részére átadni.

## Viselkedési szabályok az interneten

A felhasználóknak TILOS a Hivatalnál:

1. Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
2. fájlcserélő vagy chat szolgáltatás használata, valamint a munkavégzéshez nem kapcsolódó letöltések végrehajtása;
3. a közösségi oldalak használata, és más, a Hivataltól idegen tevékenység végzése;
4. A mindenkori hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése, tiltott haszonszerzésre irányuló tevékenység, szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
5. Egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám;
6. A Hivatal elektronikus levelezési rendszerét és a Hivatal tulajdonában lévő internet hálózatot feladatellátásain kívül másra használni;
7. A Hivatal informatikai hálózatán, eszközein a képernyőmegosztás, külföldi felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak nem kívánt levelezőlisták használata;
8. A Hivatal weboldala ellen bármiféle betörési kísérletet végrehajtani, illetve a szervezet hálózatát felhasználni más oldalak ellen elkövetett szabálysértés támogatására (kivéve a tervezett információbiztonsági ellenőrzéseket);
9. A hálózat erőforrásainak, a hálózaton elérhető adatok illetéktelen módosítása, megrongálása, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
10. A hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértében, pazarló módon igénybevevő tevékenység.

Tilos a Hivatal informatikai eszközein tárolni, feldolgozni vagy továbbítani olyan anyagokat, melyek közízlést, vagy törvényt sértenek, mint például:

1. betiltott filmeket, publikációkat;
2. számítógépes játékot;
3. pornográfiát, pedofíliát, erőszakot hirdető cikkeket, publikációkat;
4. megbotránkoztató, a jó ízlés határait sértő anyagokat;
5. gyűlöletkeltésre alkalmas, vagy vallási és kisebbségi érzelmeket sértő anyagokat.

Az informatikai kockázatok és az adatok feletti felügyelet hiánya miatt tilos nyilvános felhőalapú rendszerek használata.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrző és Internet böngésző kontrollok kiiktatása.

A Hivatal vezetője a 2011.évi CXII tv. (info tv) alapján szabályozza, ill. korlátozza az internet- és email használatot. Az internet és az IT rendszer kizárólag a Hivatalai munkát segíti, tehát kizárólag munkahelyi célra engedi használni azokat. a levelező rendszer magáncélú használatát megtiltja, ezt követően a dolgozó teljes levelezése ellenőrízhetővé válik. A Hivatal az ellenőrzés során betartja a jogviszonyban nem álló harmadik személyek személyes adatainak védelmére vonatkozó jogait.

A rendszergazda (ill. erre feljogosított, megbízott személy) jogosult ellenőrízni az internet használatát, hogy betartották-e a tiltásra vonatkozó szabályokat, valamint a hálózati kommunikációt, Hivatali levelezést az egyes IT eszközök jogos és szakszerű használatát.

Az ellenőrzések alakalmával a dolgozónak vagy általa megbízott képviselőjének joga van jelen lenni, erre a munkáltatónak kell felhívnia a figyelmét.

### E-mail biztonsági szabályok:

1. A Hivatal tulajdonát képző levelező rendszer csak Hivatali célokra alkalamzható. Magáncélra, valamint etikailag kifogásolható célokra a hivatali postafiókok nem használhatóak. Ezen túlmenően a felhasználó felel valamennyi, a címéről elküldött levél rendeltetési helyéért és annak tartalmáért.
2. Szükséges a felhasználóhoz kötött egyéni, teljes névvel ellátott, a Hivatal által használt domain nevű egyedi e-mail címek létrehozása. (gipsz.jakab@domain.hu)
3. Ha a felhasználó hosszabb időn át nem tudja postaládáját ellenőrizni, állítson be „Házon kívül” szabályt, így a feladó tudatában lesz annak, hogy a közeljövőben nem fog üzenetére közvetlen választ kapni. Ezzel egyidejűleg adja meg a helyettesítő személy nevét és elérhetőségét, hogy sürgős esetben legyen kihez fordulniuk távolléte alatt.
4. Tilos a Hivatal saját tulajdonú domain nevéhez tartozó levelezőrendszerén kívüli levelezőrendszer használata. Pl.( Freemail, Gmail)
5. Ha a felhasználó nem ismeri a külső rendszerből érkező levél feladóját, akkor az üzenet megnyitása előtt igyekezzen azt beazonosítani, gyanús esetben törölje az üzenetet, illetve jelezze ezt a felettesének vagy a rendszergazdának. Amennyiben megnyitás szükséges annak megállapítására, hogy mi az üzenet célja, úgy ezt megfelelő előrelátással tegye, és az esetleges csatolt melléklet megnyitását vírus veszély miatt feltétlenül kerülje, további címzettnek ne küldje tovább.
6. A munkavállalóknak tilos más munkavállalók postafiókjához felhatalmazás nélkül hozzáférniük
7. A munkavállalóknak tilos a tévesen címzett, másnak szóló levelek felhasználása
8. Tilos a Hivatal által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a Hivatal elektronikus levelező rendszerében létrehozott) e-mail címre
9. A kilépett munkavállaló, megszűnt szerződésű partner levelezési hozzáférését azonnal meg kell szüntetni, az érintett levelezési fiókját a rendszergazda a kilépést követően legalább 30 napig figyeli (vagy ameddig szükséges), ezt követően a fiókot meg kell szüntetni, és/vagy tartalmát más munkatárshoz rendelni.
10. Tilos a távozott munaktárs nevében elektronikus üzenetet küldeni.
11. A levelezési rendszerben a hozzáférést biztosító jelszavak létrehozására, kezelésére és változtatására vonatkozóan az általános jelszó használati szabályok érvényesek.
12. A munkatársak kötelesek a levelezési fiókjuk hozzáférését biztosító jelszót titkosan kezelni, azt mások tudomására hozni még a munkafolyamat felgyorsítása érdekében is tilos.
13. A munkatársak kötelesek azzonnal jelenteni a jelszavuk nyilvánosságra kerülésére utaló minden gyanút és körülményt.
14. Tilos a Hivatal levelezési rendszerében használt e-mail címmel magánérdekből, publikus rendszerekben regisztrálni, fórumokon megjelenni, hírlevelekre feliratkozni.
15. Tilos a Hivatal nevében olyan e-mailt küldeni, melyek:
* Bizalmas, kritikus információt tartalmaznak vagy szerződési, illetve a Hivatal ügyfeleinek érdekeit sértheti.
* A Hivatal hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatja, illetve a Hivatal ügyfeleinek érdekeit sértheti.
* Szerzői jogokat sérthetnek
* Vírusokkal fertőzhetik meg a Hivatal infrastruktúráját
* Vallási, etnikai, politikai vagy egyéb másokra nézve potenciálisan sértő, zaklató tevékenység
* Kéretlen reklámokat és hirdetéseket tartalmaznak
1. A felhasználó által küldött elektronikus leveleket a felhasználónak kell aláírnia. Nem használható önállóan csupán a Hivatal neve, vagy annak varióciói önálló aláírásként – a felhasználóknak a saját nevüket és beosztásukat kell használni aláírásként.
2. Titokvédelmi vagy egyéb biztonsági, bizalmassági okokból, amennyiben a levelek címzettjei nem szerezhetnek tudomást egymásról vagy egymás e-mail címéről, akkor a levél „Titkos másolat” („BCC”: Blind Carbon Copy) kategóriáját kell alkalmazni a címzés során.
3. A munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából, törölni/archiválni szükséges.

Levelezés a Hivatal saját tulajdonó domain nevéhez kapcsolódó tárhelyen történhet, a rendszergazda által meghatározott vagy tárhely szolgáltató által biztosított levelező rendszer használatával (lehetőség szerint (SSL) POP3 hozzáféréssel vagy webmail igény esetén (SSL) IMAP hozzáféréssel.)

 A felhasználó tudomásul veszi, hogy a Hivatal által meghatározott viselkedési szabályok megsértése fegyelmi intézkedést vonhat maga után.

## Tudatosság és képzés

### Képzési eljárásrend

A Hivatal rendszeres képzésben részesíti az információs rendszer felhasználóit. A képzések gyakoriságát az információs rendszerek változásainak és egyéb igényeknek a figyelembevételével határozzuk meg, de évente legalább egyszer belső oktatáson vesz részt minden munkavállaló. A szervezetbe újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben részesítjük. Rendkívüli oktatást tartunk a Hivatal rendszereiben történő jelentős változás vagy a Hivatal rendszereiben történő incidens után.

A Hivatal vezetése:

1. felelős a képzési kritériumok meghatározásáért
2. biztosítja a képzéshez a szükséges erőforrásokat
3. gondoskodik a képzések fontosságának tudatosításáról a teljes szervezetben

Az IBF:

1. felelős a képzési rendszer kialakításáért, fenntartásáért
2. felelős a szükséges oktatások megtartásáért, megtartatásáért

A munkatársak:

1. felelősek a képzési előírások betartásáért, a képzések során leadott anyagok elsajátításáért

### Biztonságtudatossági képzés

A jegyző felelőssége, hogy a Hivatal elektronikus információs rendszereinek felhasználói biztonságtudatossági képzések formájában megismerjék az alapvető biztonsági követelményeket. A biztonságtudatossági képzés az új felhasználók esetén már a kezdeti képzés részét képezi, továbbá a képzést legalább évente megismételjük, illetve minden olyan elektronikus információs rendszerben vagy munkakörben történő változás esetén, mely ezt indokolttá teszi.

A képzésnek kötelezően:

* felhívjuk a munkatársak figyelmét az informatikai biztonsági szabályzati rendszerben bekövetkezett változásokra
* ismertetjük azokat a sebezhetőségeket, melyek a felhasználó nem-biztonságtudatos magatartását használják ki;
* ismertetjük az azonosított, súlyosnak minősített szabálysértéseket;
* felhívjuk a figyelmet, hogy a megadott súlyos szabálysértések ismételt elkövetése milyen szankciókat von maga után.
* A szabályzatokban, jogszabályokban, szerződésekben előírt követelmények felfrissítése érdekében ismertetjük a betartandó szabályokat, kötelezettségeket, egy-egy az oktatásra kijelölt biztonsági terület esetében (pl. hozzáférés védelem témakörében a jelszókezelési szabályok stb.)

Az oktatásokon való részvétel kötelező a Hivatal informatikai rendszereihez hozzáférők számára, amely jelenlétet az oktatás végén a jelenléti ív aláírásával igazolnak.

**Alkalmazás előtt**

A jegyző feladata, hogy a Hivatal informatikai rendszereihez hozzáférő felhasználók esetén az adott feladat-, illetve munkakör betöltéshez szükséges képzettségre, tapasztalatra, gyakorlatra vonatkozó, illetve egyéb, a mindenkor hatályos jogszabályok és belső szabályozók által előírt követelmények ellenőrzése a jogviszony létesítése előtt megtörténjen, a jelölt a szükséges átvilágításon átessen.

A Hivatal informatikai rendszereihez hozzáférő minden felhasználóját munkába állását követően tájékoztatjuk az informatikai rendszerek használatára vonatkozó szabályokról, az új belépő számára biztosítjuk az informatikai biztonsági szabályok megismeréséhez és megértéséhez szükséges minden szükséges támogatást.

### Belső oktatások, továbbképzés

A jegyző feladata biztosítani, hogy a jogviszony fennállása alatt a felhasználó fenntartsa, szükség esetén megszerezze az általa ellátandó feladatkör betöltéséhez szükséges ismereteket, képzettségeket, képesítéseket, indokolt esetben biztosítsa a szükséges oktatások megtartását, illetve gondoskodjon róla, hogy a felhasználó részt vegyen a megfelelő képzéseken, továbbképzéseken.

### Képzési eljárásrend

A Hivatal a 273/2012. (IX. 28.) Korm. rendelet előírásainak megfelelően, a közszolgálati jogviszonyban foglalkoztatott munkatársak részére éves és négyéves képzési tervet állít össze. A képzések kiválasztását a felhasználók a szakterületi vezetővel egyeztetve, majd jegyzői jóváhagyással végzik. A munkavállalók szakterületüknek megfelelő képzéseken vesznek részt. A képzési tervek összeállítása a jegyző felelősségi körébe tartozik.

A kötelező képzési terven kívül a munkatársak a szakterületi vezetővel egyeztetve jegyzői jóváhagyással egyedi szakmai továbbképzéseken is részt vehetnek.

Új rendszer bevezetése esetén a jegyző felelőssége a felhasználók oktatásának biztosítása. Az új rendszerhez hozzáférés csak azoknak a felhasználóknak adható, akik részesültek a képzésben és ezt aláírásukkal igazolták.

## Fizikai Védelmi Intézkedések

## Fizikai és környezeti védelem

### Fizikai védelmi eljárásrend

A Hivatal azon helyiségeibe, ahol információs rendszerek (pl. szerverek, adatmentések, telefonközpontok, stb.) vagy rendszerelemek (pl. számítógépek) találhatóak, vagy ahonnan bármilyen jellegű hozzáférés lehetséges a rendszerekhez vagy rendszerelemekhez, csak az arra jogosultak léphetnek be, meghatározott szabályok szerint.

A szabályok és korlátozások nem vonatkoznak a létesítmény bárki által szabadon látogatható vagy igénybe vehető helyiségeire.

### Fizikai belépési engedélyek

A Hivatal:

1. összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
2. belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
3. rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
4. eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
5. intézkedik a b) pont szerinti dokumentumok visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

A Hivatal területéhez tartozó épületek, helyiségek biztonsági zónákoz töténő hozzárendelése lehetővé teszi a belépésvédelemmel kapcsolatos intézkedések hatékony végrehajtását a mindenkori védelmi igény függvényében.

Az infomrációbiztonsági felelős biztonsági zónákba sorolja a Hivatal területeit és a rendszergazda, valamint a jegyző közreműködésével meghatározza ezen területek esetében a belépésre jogosult személyek listáját, belépéshez szükséges fizikai követelményeket.

A rendszergazda a jegyző közreműködésével folyamatosan felülvizsgálja a belépésre jogosultak listáját és az érvénytelen/megszűnt jogosultásgokat eltávolítja. Jogosultságvisszavonás esetén gondoskodik a kiadott kulcsok, kártyák visszavonásáról, megsemmisítéséről, törléséről.

A kulcsokat, kártyákat olyan helyen kell tárolni, ami nem teszi lehetővé illetéktelenek számára a hozzáférést.

A Hivatal biztonsági zónái:

|  |  |  |
| --- | --- | --- |
| Zóna | Biztonsági követelmények | Helyszínek/belépésre jogosultak |
| 1. biztonsági zóna
 | Alacsony  | A Hivatal épületein belül és kívül elhelyezkedő mindazon területek, amelyek bárki (pl. ügyfél, látogató) részére nyilvánosan elérhetőek (pl. előtér, folyosó, parkoló) |
| 1. biztonsági zóna
 | Közepes | A Hivatal azon helyiségei, irodái amelyekben nincsennek elhelyezve szakfeladatot támogató elektonikus információs rendszerek (pl. tárgyalók) így ide a Hivatal minden munkatársa beléphet, illetve a látogatók, ügyfelek is kíséret és felügyelet mellett. |
| 1. biztonsági zóna
 | Magas | A Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó helyiségek (pl. ASP, anyakönyv) A belépés csak az arra jogosultak számára lehetséges, a látogatók, ügyfelek, belépése és ott tartózkodása csak a kíséret és felügyelet mellett engedélyezett. |
| 1. biztonsági zóna
 | Kritikus | IT és elláttó infrastruktúra valamennyi helyisége pl. szerverhelyiség (ideértve a szerverfunkciójú számítógépeket, adatmentő szervereket is, NTG hálózati eszközöket). A belépés kizárólag a rendszergazdának engedélyezett. Munkatársak, ügyfelek, látogatók, karbantartók, stb. kizárólag felügyelettel léphetnek be és tartózkodhatnak ott.  |

### A fizikai belépés ellenőrzése

A Hivatalnak meg kell határoznia az ügyfélforgalom számára a be és kilépési pontokat, melyet az ügyfélfogadási időn kívül zárva kell tartania, ügyfélfogadáson kívül a belépés csak felügyelet és kíséret mellett lehetséges. A nem ügyfélforgalom számára kijelölt külön bejáratokat kulccsal zárva kell tartani, a belépést csak a kiosztott kulccsal rendelkezők számára lehet biztosítani. A nyilvános területeken kívül, minden belépő ügyfelet, látogatót felügyelet alatt kell tartani, az irodákba, tárgyaló termekbe csakis kísérettel mehetnek be és tartózkodhatnak ott. A látogatót, ügyfelet fogadó munkatárs felelős a látogatóért, annak minden az információbiztonságot veszélyeztető tettéért. Azokban az esetekben, amikor az épületbe karbantartási (akár épület, akár eszköz), vagy ellenőrzési célból érkeznek, a Hivatalnak kísérnie kell ezeket a személyeket is és figyelemmel kell követnie a tevékenységüket.

A Hivatal takarítást végző szeméy/személyzet nem takaríthat felügyelet nélkül azon irodákban, ahol szakrendszeri munkaállomások vannak elhelyezve, illetve az informatikai erőforrásokat koncentrálan tartalmazó helyiségekben. (pl. szerverszoba, NTG hálózati végpont)

A Hivatal:

1. kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
2. ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
3. gondoskodik a kíséretről a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
4. megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;
5. nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
6. a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;
7. meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;
8. az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
9. felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

Az informatikai rendszereken történő adatfeldolgozás biztonsága érdekében megakadályozza az informatikai eszközökhöz történő jogosulatlan fizikai hozzáférést, illetve biztosítja az eszközök megbízható működéséhez szükséges környezeti feltételeket (pl. hőmérséklet, páratartalom érzékelő).

A jegyző felelőssége biztosítani, hogy a Hivatal helyiségeinek kialakítása, illetve az informatikai eszközök elhelyezése során a helyi adottságokat figyelembe véve elfogadható szintre csökkentse az informatikai eszközök jogosulatlan fizikai hozzáféréséből eredő kockázatokat, a lehetőségekhez képest legoptimálisabb módon biztosítottak legyenek az egyes informatikai rendszerek megbízható működéséhez szükséges környezeti és infrastrukturális körülmények.

Az 1. biztonsági zóna helyiségeinek legalább kulccsal (a kulcs ne legyen a zárban), a 2. és a 3.. biztonsági zóna helyiségeinek kulccsal vagy kóddal vagy intelligens kártyával zárhatónak kell lennie amely lehetővé teszi a biztonsági ponton való átjutás ellenőrzését, felügyeletét. A szerverhelyiségbe (3. biztonsági zóna) állandó belépési jogosultsággal nem rendelkező személyek belépésének regisztációjára szolgáló naplót a „Szerverszoba belépési nyilvántartás” tartalmazza.

Kilépés alkalmával a távozó munkavállaló kulcsát vissza kell venni amennyiben rendelkezett kóddal vagy intelligens kártyával azt tiltani szükséges.

## Alapvető normák

A felhasználók kötelesek betartani a jegyző által meghatározott fizikai védelmi intézkedéseket, önhatalmúlag nem változtathatják meg az eszközök elhelyezését, valamint kötelesek a napi munkavégzés során az alábbi alapvető viselkedési normákkal összhangban kezelni az informatikai eszközöket, illetve adathordozókat:

### A Hivatal épületén kívül

Az alábbi szabályok érvényesek minden olyan helyiségre, ami nem a Hivatal használatában, felügyeletében van. Így tipikusan ilyenek például az alábbiak:

* felhasználó lakása;
* közösségi közlekedés;
* közösségi helyek (pl. étterem, kávézó)
* egyéb közterület (pl. utca).

Az ilyen jellegű környezetben az alábbi szabályok betartásával lehet Hivatal tulajdonú informatikai eszközt tárolni, használni:

* Utcán, tömegközlekedési eszközön és egyéb nyilvános helyen a Hivatal tulajdonát képező informatikai eszközt – különös tekintettel az adathordozókra – nem szabad felügyelet nélkül hagyni.
* Ha laptopját a munkaidő letelte után hazaviszi, SOHA NE HAGYJA az autójában!
* Hivatalon kivuli és Hivatali munkavégzés során is forditsunk figyelmet arra, hogy amit billentyűzetünkön leütünk, gépelünk tehát a leütött karaktersor esetleg illetéktelenek számára látható, értelmezhető.
* Tilos bekapcsolt és bejelentkezett, de nem zárolt laptopot, vagy egyéb hordozható eszközt felügyelet nélkül hagyni.
* Laptopon, hordozható eszközökön, hordozható adathordozón a feltétlen szükséges minimumra korlátozzuk az érzékeny adatok tárolását, ahol adottak ennek a technikai feltételei lehetőség szerint az érzékeny adatokat titkosítva tároljuk (ennek egy tipikus módja, ha a laptopokon ki alakításra kerül egy titkosított partíció az érzékeny adatok tárolására)

### Üres íróasztal, tiszta képernyő politika

Az irodahelyiségekben tárolt és kezelt adatok jogosulatlan felhasználása ellen minden belépésre jogosultnak fellép. A szabályzat személyi hatálya alá tartozók

* kötelesek az általuk kezelt adathordozókat csak a használat ideje alatt maguknál tartani;
* kötelesek a papír alapú adathordozók kezelése során az iratkezelési szabályzat előírásait betartani;
* a részükre kiadott biztonsági eszközöket a hatályos szabályozások szellemében más személyek részére nem adhatják át;
* 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
* kötelesek az informatika eszközről kijelentkezni vagy azt zárolni minden esetben, ha a tevékenységet befejezte vagy megszakítja oly módon, hogy az informatikai eszköz felügyelet nélkül marad;
* a zárolás elfelejtésének esetére jelszóvédett, automatikus zárolást kell beállítani, úgy, hogy az maximum 10 perc inaktivitást követően zárolja a számítógépet;
* kötelesek minden esetben a harmadik felek felügyeletéről gondoskodni, annak érdekben, hogy az ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz;
* a munkanap végén a rendelkezésére bocsátott informatikai eszközt kikapcsolni. Ez alól a szabály alól a jegyző személyre, eszközre, munkafolyamatra vonatkozó felmentést adhat, ha ez szakmailag indokolt.

### Látogató kísérete

Az irodahelyiségekben harmadik személy nem tartózkodhat felügyelet nélkül, az üres irodákat bezárjuk, annak érdekben, hogy ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz.

Látogató fogadásakor a látogató felügyeletét az irodahelyiségben a felhasználónak biztosítja. Az irodahelyiségben a látogatóért a felhasználó felelősséggel tartozik.

### A kiemeneti eszközök hozzáférés ellenőrzése

A fénymásoló és nyomtató berendezéseket/multifunkciós eszközöket, a fax készülékeket és minden egyéb kimeneti eszközt védett területen belül kell elhelyezni, ahol a felügyeletük biztosítható, illetve az illetéktelen hozzáférés megakadályozható. A kinyomtatott vagy másolt dokumentumokat, fax-ot nem szabad őrizetlenül az eszközökben hagyni. A hibásan nyomtatott, nem használt dokumentumokat meg kell semmísíteni (pl. iratmegsemmísítő).

A képernyőket úgy kell elhelyezni, hogy azok minél kevesebb lehetőséget biztosítsanak illetéktelen személyek betekintésére.

### Behatolás riasztás, felügyeleti berendezések

A Hivatal egész épületére érvényes, hogy azt behatolást riasztó berendezéssel kell ellátnia, amely esetében gondoskodni kell a távfelügyeletre való bekötésről. A Hivatal rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat.

### Áramellátó berendezések és kábelezés

A Hivatalnak meg kell védenie az elektonikus információs rendszert árammal ellátó berendezéseket, valamint a kábelezést a sérüléssel és rongálással szemben. Az elsődleges áramforrás kiesése esetére a 3. biztonsági zónában lévő eszközök szabályos leállításához a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást kell biztosítani (különös tekintettel az NTG hálózati eszközökre).

### Vészvilágítás

A Hivatal egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

### Tűzvédelem

A Hivatalnak az elektronikus rendszereknek helyt adó irodákban/helyiségekben/szerverszobában független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket szükséges alkalmaznia, és karban tartania. Ezen kívül a folyosókon, illetve ahol tűzvédelmi szempontból indokolt, tanúsított porral oltó készülékeket kell tartani.

### Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

A Hivatalnak védeni kell a 2. és 3. biztonsági zónában lévő elektronikus információs rendszereket/rendszerelemeket a csővezeték rongálódásából származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. szerverszoba, NTG végpont) során biztosítani kell, hogy az a víz és más hasonló kártól védett legyen, ha szükséges akár a csővezetékek kiváltásával, áthelyezésével is. Ezekben a helyiségekben közvetlenül felettük vizesblokk kialakítása tilos.

### Hőmérséklet és páratartalom ellenőrzés

A szerverhelyiségben elhelyezett központi kiszolgáló egységek biztonságos működése érdekében a hőmérsékletet 22-24 Celsius fok között kell tartani.

A hőmérsékletet az elhelyezett eszközök hő leadását figyelembevevő teljesítménnyel rendelkező klímaberendezéssel kell biztosítani.

A klímaberendezés által termelt kondenzvizet erre rendszeresített zárt csatornán ki kell vezet-ni a szerverhelyiségből.

A relatív páratartalom szintjét 40-60% között kell tartani. A hőmérsékletet és a relatív páratartalom szintjét arra alkalmas eszközzel folyamatosan mérni kell. Az eszköznek riasztást kell adnia (pl.: SMS, email) a rendszergazdának, hogy ha a hő-mérséklet 18 Celsius fok alá csökken vagy meghaladja a 28 Celsius fokot, illetve ha a relatív páratartalom szintje eléri a fent megadott határértéket. Felelős: Rendszergazda

### Be- és kiszállítás

A rendszergazda engedélyezi, vagy tiltja a létesítménybe bevitt, onnan kivitt információs rendszerelemeket. A Hivatal tulajdonában lévő kiadott eszközökről átvételi elismervényt kell írni amely egyértelműen tartalmazza a kiadott eszköz jellemzőit és a kiadással járó felelősségeket. Az eszköz visszaszolgáltatásakor a rendszergazdának meg kell győződni arról, hogy az megfelel a kiadáskori állapotának.

Az eszközök igénylését a megbízott szervezeti egység vezetőhöz vagy a rendszergazdához kell benyújtani.

Behozott eszköz esetében az üzembehelyezést megelőzően meg kell vizsgálni az eszközt, hogy megfelel-e a munkavégzéshez szükséges követelményeknek, információbiztonsági elvárásoknak. Amennyiben az eszköz nem felel meg az elvárt követelményeknek, úgy nem engedélyezhető a Hivatal belső hálózatára való csatlakoztatása.

A behozott eszköz munkahelyi használatból való kivonását megelőzően a rendszergazdának át kell azt vizsgálnia, hogy nem tartalmaz-e munkavégzés során keletkezett bizalmas, illetve egyéb adatokat.

A redszergazda a kiadott/behozott eszközökről nyilvántartást kell, hogy vezessen.

A nyilvántartás legalább az alábbiakat tartalmazza:

* eszköz megnevezése (pl. notebook, pendrive, telefon, stb.)
* szériaszám, modell
* kinek adta ki/ki hozta vissza
* mikor adta ki, mikor hozta vissza, mikor hozta be, mikor viszi el
* alapkonfiguráció (operációs rendszer, szoftverek, stb.) ahol értelmezhető
* ellenőrzés eredménye (pl. a visszahozott eszköz megfelel a kiadáskori állapotának, a korábban behozott eszköz nem tartalmaz munkavágzésből származó adatokat)
* szükgséges intézkedések (pl. telepítés, frissítés, törlés, javítás)
* aláírás (rendszergazda, munkatrs, harmadik személy)

Eszköz szervizbe történő szállítása esetén jegyzőkönyvet kell készíteni, és a rendszergazdának az adathordozókra vonatkozó adatvédelmi szabályoknak megfelelően kell eljárnia. A szerviz által kiadott szállító levelet a rendszergazdának szükséges megőriznie.

### Karbantartók

A külső szolgáltatóknak, illetve karbantartást végző személynek meg kell ismernie a Hivatal információbiztonsági előírásait és titoktartási nyilatkozatot kell aláírnia.

A karbantartást csak az arra kijelölt személyek végezetik el akik névsora szerepel a létrejött szerződéses megállapodásban illetve az eszközhöz, rendszerekhez, szükséges karbantartási jogosultságok meghatározásra került. A szerződésben ki kell kötni, hogy személyi változás esetén, haladéktalanul tájékoztatást kell küldeni a Hivatalnak.

A Hivatalba történő belépéshez, a karbantartási feladatok ellátásához a személyazonosságot igazolni szükséges (külső karbantartók esetében). E nélkül a belépés nem lehetséges. Az eszközök, rendszerek karbantartási munkálatait külső karbantartók esetében a rendszergazdának felügyelni szükséges, hogy kizárásra kerüljenek a jogosulatlan hozzáférések, illetve hibás karbantartási tevékenységek.

A hibákat, rendszerleállásokat, minden karbantartási tevékenységet dokumentálni kell.

A rendszergazdának nyilvántartást kell vezetnie a karbantartó szervezetekről/személyekről elérhetőségeikről azok jogosultságairól és arról, hogy mit tartanak karban és ezt változások esetén aktualizálnia kell.

### Időben történő javítás

A biztonsági követelmények teljesítése érdekében az elektronikus információs rendszerelemek (eszközök) karbantartásáról gondoskodni kell. Gondoskodni kell arról, hogy az elektronikus információs rendszerelemek időben történő javítása megtörténjen. Ehhez szükséges tudatosítani a felhasználókban a hiba/eltérés időben történő jelentését, illetve naprakészen kell tartani a karbantartást végzők nyilvántartását, azok elérhetőségeit és azonnal fel kell venni velük a kapcsolatot a mielőbbi elhárítás érdekében.

A karbantartást csak az arra kijelölt személyek végezhetik el.

## Logikai Védelmi Intézkedések

### Általámnos védelmi intézkedések

### Személyi biztonság

A Hivatal:

1. megfogalmazza, dokumentálja, valamint kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;
2. Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;
3. legalább évente felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását;
4. gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;
5. meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket;

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

### Az elektronikus információs rendszer kapcsolódásai

Szabályozni kell és szükség esetén belső engedélyhez kell kötni az elektronikus információs rendszerek kapcsolódását más elektronikus információs rendszerekhez, dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektonikus infomrációk típusát.

Az összekapcsolást a jegyzőnek, rendszergazdának, valamint az IBF-nek is jóvá kell hagynia.

Más kapcsolódó szervezet csak a Hivatal által nyújtott interfészen keresztül csatlakozhat a Hivatal elektronikus információs rendszereihez. Szabványos, sérülékenységektől mentes kriptográfiai eszközökkel gondoskodni kell az átvitt adatok bizalmasságának és sértetlenségének biztosításáról. Az összekapcsolás feltételeinek fennállását legalább évente ellenőrizni kell.

Belső rendszer kapcsolatok:

az érintett szervezet belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását;

A Hivatal elektronikus információs rendszere több elemből épül fel, melyek bizonyos interfé-szeken kapcsolódhatnak egymáshoz. Valamennyi interfészt dokumentálni kell.

Külső kapcsolódásokra vonatkozó korlátozások:

Szabályrendszert kell felállítani és alkalmazni a külső elektronikus információs rendszerekhez való kapcsolódásokhoz, amelyek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

A Hivatal határvédelmének működtetése során alapértelmezés szerint minden kapcsolatot tiltani kell, csak a működéshez szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Amennyiben az értelmezhető, úgy az érintett kapcsolatnál IP alapú korlátozást kell bevezetni és gondoskodni kell a megfelelő azonosításról és hitelesítésről, valamint az átvitt adatok sértetlenségéről, rendelkezésre állásáról és bizalmasságáról. Valamennyi interfészt dokumentálni kell. Felelős: Rendszergazda

## Tervezés

### Rendszerbiztonsági terv

A Hivatal vezetése az elektronikus információs rendszereihez rendszerbiztonsági tervet készített, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik:

1. összhangban áll az Informatikai Biztonságpolitikával, valamint igazodik a szervezet felépítéséhez és architektúrájához,
2. meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait és azok elvárt szolgáltatási szintjeit [angolul SLA]), biztonságkritikus elemeit és alapfunkcióit;
3. meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
4. meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
5. a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit (naplózás, mentés és helyreállítás, üzletmenet-folytonosság);
6. meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és azok bővítését, végrehajtja a jogszabály szerinti biztonsági feladatokat;
7. gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
8. belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét (belső audit);
9. frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
10. elvégzi a szükséges belső egyeztetéseket;
11. gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A rendszerbiztonsági tervet a rendszergazda készíti el az IBF közreműködésével.

### Cselekvési terv

A Hivatal cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;

a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;

frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

A jegyző felelőssége biztosítani az elektronikus információs rendszerek biztonságáért felelős személy szakmai támogatása mellett a cselekvési terv előrehaladásának folyamatos nyomon követését és a fontosabb mérföldkövek mentén a feladatok előre haladásának értékelését. A jegyző elrendelheti, illetve az elektronikus információs rendszerek biztonságáért felelős személy kezdeményezheti a készre jelentett feladatok utóvizsgálatát, amit utólag beépítünk az éves ellenőrzési tervbe.

Ha a cselekvési terv feladatainak előrehaladásában a cselekvési terv végrehajtását veszélyeztető probléma jelentkezik, akkor a jegyző feladata rendelkezni a probléma kezelésének módjáról, szükség esetén a cselekvési terv átütemezéséről.

### Személyi biztonság

A Hivatal megfogalmazta, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;

* az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;
* meghatározott gyakorisággal felülvizsgálja, és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását;
* gondoskodik arról, hogy a változás esetén az eljárás szerinti frissítés, aktualizálás megtörténjen;
* meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket

## A rendszer fejlesztési életciklusa

A Hivatal az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket.

A Hivatal a fejlesztési életciklus egészére meghatározza és dokumentáltatja az információbiztonsági szerepköröket és felelősségeket.

A Hivatal meghatározza és a Hivatalra érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

### A rendszer életciklus szakaszai a következők:

1. követelmény meghatározás;
2. fejlesztés vagy beszerzés;
3. megvalósítás vagy értékelés;
4. üzemeltetés és fenntartás;
5. kivonás (archiválás, megsemmisítés).

### Sérülékenység-teszt

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő elektronikus információs rendszerek esetében, amennyiben az adott elekronikus információs rendszer rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik, külső szervezet bevonásával gondoskodik a rendszer sérülékenységi vizsgálatának elvégzéséről az elekronikus információs rendszer üzembe helyezését megelőzően, illetve új, lehetséges sérülékenységek felmerülésekor.

## Konfigurációkezelés

### Konfigurációkezelési eljárásrend

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központilag tárol információkat így segíti az incidensfelügyeletet, problémakezelést, változáskezelést és a verziókövetést.

A konfiguráció megváltozását az rendszergazda minden esetben köteles dokumentálni a hardver és szoftver komponensekről vezetett nyilvántartásban, illetve az érintett rendszer dokumentációjában vagy a rendszer üzemeltetési leírásában.

Minden változtatást jóvá kell hagyatni a Jegyzővel.

### Elektronikus információs rendszerek nyilvántartása

A jegyző felelőssége, hogy a Hivatal teljeskörű, naprakész nyilvántartást vezessen a Hivatalban használt elektronikus információs rendszerekről. A nyilvántartás tartalmazza az elektronikus információs rendszer:

* nevét;
* funkcióját;
* nyújtott szolgáltatását;
* licencszámát;
* szakterületi felelőst és elérhetőségét;
* üzemeltetési felelőst és elérhetőségét;
* továbbá releváns esetben a külső elérhetőségeket.

A rendszergazda feladata a nyilvántartás elkészítése és az évente történő felülvizsgálata.

### Elektronikus információs rendszerelem leltár

Az elektronikus információs rendszerelem leltár a Hivatal hardver- és szoftvernyilvántartása. A nyilvántartás elkészítése és naprakészen tartása a rendszergazda feladata.

A nyilvántartásunk kiterjed:

* az informatikai eszközök leltári és műszaki adataira;
* az informatikai eszközökre telepített szoftverekre, azok licencnyilvántartására, külön rögzítve;
	+ a megvásárolt licenceket;
	+ Hivatal megrendelésére fejlesztett termékek licenceire.

Az informatikai eszközök, illetve azok használatát érintő változások szabályozott keretek között történő végrehajtását az elektronikus információs rendszer biztonságáért felelős személy időszakosan ellenőrzi.

### Alapkonfigurációs nyilvántartás

A Hivatal által használt desktopok, laptopok és szerverek valamint hálózati elemek és az egyes elemek közötti logikai kapcsolatok esetében egy alapkonfigurációs nyilvántartást készítünk, és folyamatosan aktualizálunk. A nyilvántartás elkészítéséért és frissítéséért a rendszergazda felel.

A nyilvántartásnak legalább az alábbi tételeket tartalmazza:

* alapértelmezett hardver;
* alapértelmezett operációs rendszer;
* alapértelmezetten telepítendő programok;
* alapértelmezett alkalmazott policy beállítások;
* alkalmazandó biztonsági beálltások;

Változások esetén azonnal, de legalább évente szükséges a nyilvántartás felülvizsgálata. A felülvizsgálat rendszeres végrehajtásáért az elektronikus információs rendszer biztonságáért felelős személy felel.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett elektonikus információs rendszerek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott elektronikus információs rendszer használatához szükséges konfiguráció tartalmát, a kompatibilitási, illetve a minimális hardver- és szoftverkövetelményeket és ezek beállításait.

### A konfigurációváltozások felügyelete (változáskezelés)

A Hivatal konfigurációváltozás esetén gondoskodik a változás hatásainak vizsgálatáról, valamint a változtatásra vonatkozó döntés dokumentálásáról.

A változtatás végrehajtása az engedély birtokában a kijelölt felelős (pl.: rendszergazda) feladata. A változtatást a rendszergazda hardver és szoftver komponensek esetében az elektonikus információs rendszerelem leltárban, beállítások módosítása esetén az érintett rendszer dokumentációjában, illetve a rendszer üzemeltetési leírásában köteles rögzíteni.

Az információbiztonsági felelős jogosult a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységek ellenőrzésére, illetve felülvizsgálati tevékenysége során – minimum éves rendszerességgel – auditálja azt.

### Előzetes tesztelés és megerősítés

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő elektonikus információs rendszerek esetében a konfiguráció megváltoztatása előtt hajtja végre és engedélyezi, valamint dokumentálja a változást.

A teszt környezet jogosultsági beállításai, jogosultságkezelési folyamatai és adatbiztonsága az éles rendszerrel megegyező elvárásokat kell, hogy teljesítse. A teszt adatbázist teljes mérték-ben az eredetivel megegyező módon kell kezelni, a hozzáférés szabályozást is beleértve.

A tesztelést dokumentált formában kell végezni, a tesztek eredményeit dokumentálni kell, amely alapul szolgál a változtatás éles környezetben történő átvezethetőségére.

Hardver meghibásodás miatt szükséges rendszerelem csere esetében a beépítésre kerülő új hardverelem műszaki megfelelőségének vizsgálata az rendszergazda feladata. Karbantartás, illetve hibajavítás céljából kizárólag olyan hardverelem építhető be, amely a használt elektronikus információs rendszerek ismert kompatibilitási és konfigurációs igényeinek megfelel.

### Biztonsági hatásvizsgálat

A változtatás megkezdése előtt az IBF-nek egy előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható kockázatainak minimalizálását. A kockázatelemzésnek ki kell terjedni minden olyan lényeges elemre, amely rávilágíthat a változtatás következtében bekövetkező biztonsági problémákra.

### A szoftverhasználat korlátozásai

A Hivatal:

1. kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak; Az eredeti példányt biztonságos helyen kell tárolni.
2. a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
3. ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.
4. a Hivatal eszközein szoftvereket (beleértve a hozzájuk tartozó dokumentációt) csak a felhasználási jog keretei szerint szabad telepíteni, másolni, futtatni, kivéve a törvény adta szabad felhasználás körében (így különösen biztonsági másolat készítése céljából). Egyetlen termék többszörös használata esetén a szoftver csak a licenc megállapodásnak megfelelően használható. A Hivatal informatikai eszközeire TILOS illegális és/vagy nem jogtiszta szoftvert telepíteni!
5. a Hivatal informatikai eszközeire szoftvereket a rendszergazda telepíthet, és olyan logikai biztonsági megoldásokat alkalmazunk, mellyel biztosítható hogy rajta kívül más rendszerfelhasználó ne legyen képes programtelepítésekre.
6. az informatikai rendszerek üzemeltetési feladataival megbízottak felelőssége, hogy csak akkor telepítsenek licencköteles programot informatikai rendszerre, ha előzetesen meggyőződtek róla, hogy azzal szerzői jogot, licenc megállapodást nem sértenek, a program jogszerű használatát igazoló bizonylatok, okiratok rendelkezésre állnak.
7. a rendszergazda feladata rendszeres időközönként (legalább évente) ellenőrizni automatikus, vagy manuális módszerekkel a hivatali szoftverhasználat jogtisztaságát, illetve szerzői jogvédett tartalmak (pl. zene, film, dokumentumok) jogosulatlan megosztását a Hivatal informatikai rendszerein.
8. illegális szoftverek használata, illetve a Hivatal által nem engedélyezett szerzői jogvédett tartalmak tárolása esetén a használatban és megosztásban érintett felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat, mely eljárást az informatikai feladatokért felelős vezető kezdeményezheti a jegyző felé.
9. Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből.

### A felhasználó által telepített szoftverek

A Hivatal a dolgozóinak, felhasználóinak hardveresen nem, szoftveresen korlátozza a telepítési és módosítási jogosultságokat, valamint azokat szabályban tiltja. A Hivatal rendszereire, valamint azok számítógépeire és egyéb komponenseire csak a rendszergazdák, vagy megbízottak telepíthetnek szoftvereket, valamint azok rendszerszintű beállításait is csak ők (vagy az általuk megbízott külsős szakértők) jogosultak megváltoztatni.

Amennyiben technikai okok miatt rendszergazdai jogokkal rendelkezik a felhasználó akkor sem jogosult munkahelyi vezetője vagy a rendszergazda engedélye nélkül hardver vagy szoftver telepítése, módosítása.

### Legszűkebb funkcionalitás

A Hivatal:

* az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;
* meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

## Karbantartás

### Rendszer karbantartási eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

### Rendszeres karbantartás

A Hivatal által megbízott személyek vagy vállalkozók:

1. a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
2. jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
3. az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;
4. az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
5. ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
6. csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási a számítástechnikai eszközökön javítást, módosítást, illetve új eszközök telepítését csak a rendszergazdák, vagy az általuk megbízott és ellenőrzött külső vállalkozó végezhet;
7. számítógépek esetében, ha a javítás külső helyszínen történik, az esetleges adattartalmat töröljük, az el- és visszaszállítást pedig dokumentáljuk
8. a nem javítható eszközöket a leírtaknak megfelelően selejtezzük, esetleges adattartalmukat pedig – szükség esetén véglegesen és helyreállíthatatlanul – töröljük
9. a tervezett karbantartások mértéke és gyakorisága megfelel a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer elvégzésre kerül;
10. minél nagyobb mértékben járuljon hozzá a kockázatok (a működési szabályok betartásával) csökkentéséhez, a helyes és rendszeres karbantartottság révén;

### Tervezett karbantartások

A Hivatal az eszközparkot az alábbi gyakorisággal tartja (vagy tartatja) karban, melyek elvégezését és eredményét dokumentálja:

Hivatali számítógépek: ezen eszközökön a rendszerfrissítések automatikusan megtörténnek, azok felhasználói beavatkozást nem igényelnek. Ennek ellenőrzéséért a rendszergzada a felelős. Az elmaradt frissítések okát felderíti és pótolja azokat.

Szerverek: évenkénti karbantartás, amely tartalmazza az operációs rendszer ellenőrzését, valamint a szerver teljes újraindítását. A patch-ek futtatása havonta történik, kivétel képez ez alól azon frissítések futtatása, amelyeket a rendszer fejlesztője kritikus hibák javítására bocsájt ki, ebben az esetben a frissítést azonnal el kell végezni.

Számítástechnikai hálózat: évenkénti karbantartás és tesztelés, amely magába foglalja a hálózati eszközök újraindítását, működésének ellenőrzését. Hiba esetén feltárja annak okát, amennyiben szükséges, felveszi a kapcsolatot a szervizelésre jogosult partnerrel.

Nyomtatók és egy eszközök: igény szerinti, de legalább évente, amely magába foglalja az eszközök újraindítását, működésének ellenőrzését. Hiba esetén feltárja annak okát, amennyiben szükséges, felveszi a kapcsolatot bérelt eszköz esetén a szolgáltatóval, hivatali tulajdonú eszköz esetén a szervizelésre jogosult partnerrel.

A karbantartási tervet, valamint a karbantartásról készült feljegyzéseket az Alapkonfiguráció.xlsx – Karbantartás füle tartalmazza.

### Távoli karbantartás

A Hivatal:

* jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;
* akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;
* hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;
* nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;
* lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

### Adathordozók védelmére vonatkozó eljárásrend

A Hivatal jelen eljárásrendjében rögzíti az adathordozók védelmére vonatkozó előírásait.

Az adathordózónak minősülő eszközök (pl. floppy, CD, DVD, USB eszközök, külső merevlemezek, stb.) kezelésének a Hivatalban használatos irányelvei:

1. hozzájárul az adathordozók kezeléséből eredő kockázatok csökkentéséhez;
2. lehetővé teszi valamennyi, a tevékenységet érintő adathordozók kezelésével kapcsolatos fenyegető esemény azonosítását;

A munkavégzéshez a Hivatal tulajdonában lévő, nyilvántartott adathordozót lehet használni. Az adathordozó használatára való igényt a rendszergazdához kell benyújtani.

A Hivatal ügyviteli folyamataihoz, valamint a rendszergazda által használt külső adattárolóiról (pl. flash disk, USB pendrive, memóriakártya, hordozható HDD és SSD) a rendszergazda nyilvántartást vezet.

Adatot adathordozón/mobil eszközön (laptop, pendrive, CD/DVD, stb.) a Hivatalból kijuttatni csak a jegyző írásos engedélyével szabad az információbiztonsági előírásoknak megfelelően.

### Adathordozók használata

A Hivatal engedélyezi az adathordozók használatát, és dokumentálja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint jogosítványuk tartalmát, időtartamát.

A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

### Hozzáférés adathordozókhoz

Az adathordozókat alapértelmezetten a rendszergazda tárolja és tartja nyilván. A rendszergazda bocsájtja rendelkezésre az adathordozókat igény esetén meghatározott időre. Ettől az eljárástól eltérni csak a Jegyző engedélyével lehet.

A használni kívánt adattárolót a tárolásra kijelölt helyről vesszük ki és használatot követően oda is helyezzük vissza. A munkaasztalokon csak a munkavégzéshez használatos adathordozók lehetnek. Tilos az adathordozókat nyilvános helyen vagy harmadik félnél történő munkavégzés során őrizetlenül hagyni.

Az adattárolóknak minden felhasználónak rendeltetésszerűen használja. A Hivatal adathordozóin csak munkavégzéshez szükséges adatokat tároljuk.

Amennyiben kívülről érkezik adat valamilyen adathordozón, annak megtekintése csak előzetes ellenőrzés és vírusszűrés után használható.

A Hivatalból kilépő munkatársak vagy szerződéses viszony esetén a szerződés megszűnésében érintett megbízott harmadik felek kötelesek minden a birtokukban vagy használatukban lévő, a Hivatal tulajdonát képző eltávolítható adathordozót a rendszergazdának biztonságosan átadni, aki ellenőrzi, hogy az adathordozó állapota megegyezik-e a kiadáskori állapotával.

### Kriptográfiai védelem

Minden olyan hordozható eszközt, (pl. pendrive, notebook, stb.) amelyet a Hivatal területén kívül használnak, szállítanak kriptográfiai mechanizmusokkal kell védeni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének védelme érdekében.

### Adathordozók törlése

A meghibásodott, további felhasználásra alkalmatlan adathordozókat a rendszergazdának fizikai roncsolással megsemmisíti.

Az adathordozókat selejtezés vagy az újrafelhasználásra való kibocsátás előtt a rendszergazdának helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli, így védve az adatok bizalmasságát. A biztonságos törlés eredményességét a rendszergazdának minden esetben ellenőrzi. Azokat az adathordozókat, amelyeket nem lehet biztonságosan törölni, újrafelhasználni tilos és meg kell semmisíteni.

### Vagyontárgyakért viselt felelősség

A jegyző felelőssége, hogy a Hivatal informatikai rendszerein kezelt adatok, az azokat tároló adathordozók, illetve az azokat kezelő informatikai eszközök védelme a kezelt, illetve feldolgozott adatok érzékenységének és a kapcsolódó jogszabályi követelményeknek megfelelő módon valósuljon meg, értékelje az adatok informatikai eszközökön történő feldolgozásának kockázatait és a kockázatok elfogadható szinten tartásának figyelembe vételével alakítsa ki az ügyviteli, adatvédelmi, illetve informatikai biztonsági szabályokat. A jegyző felelőssége, hogy a selejtezés a rendszergazda bevonásával történjen és minden leselejtezett, de nem megsemmisített adathordozót a Hivatal elzártan tároljon. Az adathordozók megsemmisítése során olyan eljárást alkalmazunk, mely biztosítja az adattartalmuk visszaállíthatatlanságát.

## Informatikai nyilvántartások

Az Ibtv. előírásainak megfelelően a Hivatal naprakész nyilvántartást vezet a Hivatal elektronikus információs rendszereiről. Felelős: Rendszergazda

## Azonosítás és hitelesítés

### Azonosítási és hitelesítési eljárásrend

A Hivatal vezetése megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

### Azonosító kezelés

A Hivatal:

1. az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a Hivatal által meghatározott személyek vagy szerepkörök jogosultságához köti;
2. hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;
3. meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását
4. meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.

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

### A hitelesítésre szolgáló eszközök kezelése

A Hivatal vezetése által kijelölt személy:

1. ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
2. meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
3. biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
4. dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
5. megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
6. meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
7. a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
8. megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
9. megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
10. lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

### Jelszó (tudás) alapú hitelesítés

A Hivatal a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja;

### Birtoklás alapú hitelesítés

A Hivatal:

* az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel a Hivatal által meghatározott minőségi követelményeknek, vagy
* az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal.

Az önkormányzati ASP rendszer csak e-személyi használatával és jelszó alapú azonosítás és hitelesítés után érhető el. Az e-személyi tartalmazza a birtokláshoz szükséges adatokat (magán kulcs és egyéb azonosító adatok). Kiemelt figyelmet kell fordítani az e-személyi megőrzésére.

**Személyes vagy megbízható harmadik fél általi regisztráció**

A Hivatal meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le a Hivatal által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

### A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

### Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett hivatalon kívüli felhasználókat és tevékenységüket.

Külső partnerek (szerződött partnerek, harmadik személyek) vonatkozásában a Hivatal IT rendszereihez való hozzáférés csak a szerződés alapján biztosítható.

Külső partnerek esetén a hozzáférési jog maximum a szerződés jelártáig adható. A Hivatal IT rendszereihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés/megállapodás és titoktartási nyilatkozatok alapján gyakorolhatják.

### Hitelesítésszolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

## Hozzáférés ellenőrzése

### Hozzáférés ellenőrzési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

### Felhasználói fiókok kezelése

A Hivatal:

1. meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;
2. kijelöli a felhasználói fiókok fiókkezelőit;
3. kialakítja a csoport- és szerepkör tagsági feltételeket;
4. meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;
5. létrehozza, engedélyezi, módosítja, letiltja, és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
6. ellenőrzi a felhasználói fiókok használatát;

…értesíti a fiókkezelőket, ha:

1. a felhasználói fiókokra már nincsen szükség;
2. a felhasználók kiléptek vagy áthelyezésre kerültek;
3. az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

…feljogosít az elektronikus információs rendszerhez való hozzáférésre:

1. az érvényes hozzáférési engedély,
2. a tervezett rendszerhasználat,
3. az alapfeladatok és funkcióik alapján;

A Hivatal évente vagy a fiók és vagy felhasználó változása esetén felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot. Felelős: Rendszergazda

A megbízott személy kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök, adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

### Legkisebb jogosultság elve

Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

### Privilegizált fiókok

A Hivatal az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

### Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

### Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Nincsenek olyan felhasználói tevékenységek, melyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül végre lehetne hajtani.

### Külső elektronikus információs rendszerek használata

A Hivatal és a külső rendszer működtetője meghatározza, hogy:

1. milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;
2. külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Hivatal által ellenőrzött információkat.
3. külső szolgáltató a Hivatali rendszeren, azonosítatlan és engedéllyel nem rendelkező tevékenységet nem végezhet.
4. A Hivatal, semmilyen külföldi felhő-alapu tárhelyszolgáltatást a nemzeti adatvagyon védelme érdekében nem vehet igénybe, azt technikailag nem teszi lehetővé (pl. dropbox, gmail, drive) Ettől eltérően csak a NEIH rendelkezhet, annak írásos engedélyéhez köti.

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (E-ügyintézési tv.) szerinti szabványos információátadási felületeket a Hivatal Információátadási Szabályzata tartalmazza.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett elektronikus információs rendszerek esetében a Hivatal a rendszer tulajdonosa által meghatározott feltételeket és szabályokat alkalmazza.

Külső rendszerből való hozzáférés esetén is biztosítani kell azokat a feltételeket, amelyeket a Hivatal a hivatali belső rendszerek biztonsága érdekében megvalósít (pl. naprakész operációs rendszer, naprakész víruskereső, tűzfal, biztonságos protokoll használata, stb.)

### Nyilvánosan elérhető tartalom

A Hivatal:

1. kijelöli a Hivatal vezető beosztású munkatársát, aki jogosult a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivataltól kapcsolatos bármely információ közzétételére;
2. a kijelölt személyt képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;
3. közzététel előtt átvizsgálja a javasolt tartalmat;
4. meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.
5. A Hivatal nyilvánosan elérhető rendszerként definiálja például a Hivatal publikus weboldalát.
6. A publikus felületeken való közzétételt és a médiával való kommunikációt a jegyző szabályozza, a Hivatal külső kommunikációjáért a jegyző a felelős.
7. A Hivatali honlap (domain.hu) tartalommenedzsmentjét a rendszergazda vagy a jegyző által megbízott személy végzi.
8. A hivatali ügyintézéssel kapcsolatos dokumentációk, határozatok, rendeletek a jegyző, illetve a polgármester jóváhagyását követően kerülnek nyilvánosságra.
9. A publikált információk csak nyilvános adatokat és információkat tartalmazhatnak. A jegyző legalább évente áttekinti a honlapot és nem nyilvános adat (pl. személyes adat) kikerülése esetén eltávolítatja azt.

Az informatikabiztonsági felelős időszakos ellenőrzés keretében szintén ellenőrzi a honlap tv-nek való megfelelését.

Amennyiben a Hivatali honlap, külsős adatokat felhívásokat, egyéb információkat tartalmaz, annak valódiságtartalmáért a külsős által megadott (vagy felhelyezett) adatok tartalmáért a külsős tárhelybérlő a felelős. A jogszabályba vagy közerkölcsbe ütköző adatok információk kihelyezését megtagadjuk.

### Munkaszakasz zárolása

Az informatikusnak meghatározott időtartamú (10 perc) inaktivitás után képernyővédelmet kell beállítani a munkaállomásokra a jogosulatlan használat elkerülése végett. Felhasználói inaktivitást követően a képernyőkímélőnek pár percen belül automatikusan zárolnia kell a munkaállomást. A munkaszakasz folytatása kizárólag a felhasználó azonosításával és hitelesítésével történhet.

### Képernyőtakarás

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni.

### A munkaszakasz lezárása

Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt a Hivatal által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után. A felhasználó a munkaidő végeztével köteles a munkaállomását kikapcsolni.

**Vezeték nélküli hozzáférés**

A Hivatal:

* belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket ad ki a vezeték nélküli technológiák kapcsán;
* engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Valamennyi hozzáférési pontot a Hivatal által biztosított központi kontrolleren kell létrehozni. Gyári beállításokat a telepítés során meg kell változtatni, különös tekintettel a menedzsment felület elérésére, valamint a beépített felhasználókra és jelszavakra.
Az eszköz sugárzási tartományát úgy kell megtervezni, hogy – a lehetőségek szerint – minimális legyen a lehetőség a hálózat Hivatal épületein kívüli elérésére, azaz az épület fizikai határait ne lépje át a kiszolgálási terület. Biztosítani kell a hozzáférési pontok felügyeletét. A Hivatalban ad-hoc Wi-Fi hálózat nem létesíthető. Felelős: Rendszergazda

**Mobil eszközök hozzáférés ellenőrzése**

A Hivatal:

* belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket ad ki az általa ellenőrzött mobil eszközökre;
* engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

A Hivatal a felhasználók hivatali és saját mobil eszközei részére nem engedélyezi a Hivatali hálózathoz történő csatlakozást.

**Titkosítás**

A Hivatal teljes eszköztitkosítást, tároló alapú titkosítást vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

## Rendszer- és információsértetlenség

### Rendszer- és információsértetlenségére vonatkozó eljárásrend

A rendszer- és információsértetlenség megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el.

A fentieken túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszerek és információk sértetlenségének megőrzése érdekében:

### Hibajavítás

A Hivatal:

1. azonosítja, belső eljárásrendje alapján jelenti és kijavítja, vagy kijavíttatja az elektronikus információs rendszer hibáit;
2. telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;
3. a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepíti, vagy telepítteti;
4. beépíti a hibajavítást a konfigurációkezelési folyamatba.

A sebezhetőségek elkerülése érdekében a rendszerek sebezhetőségeit jelentős késedelem nélkül, tervszerűen és ellenőrzött módon ki kell javítani a gyártók által biztosított frissítések, patchek használatával. Az operációs rendszerek verzó frissítése csakis előre megtervezett módon történhet. A biztonságkritikus szoftvereket a rendszergazdának a frissítésük kiadását követően telepíteni szükséges. (a frissítések történhetnek automatikusan is az operációs rendszer frissítési beállításainak megfelelően.)

A változást előzetesen tesztelni szükséges egy a Hivatali környezethez hasonló teszt rendszerben minden kritikus szolgáltatás és alkalmazás vonatkozásában a kompatibilitás és az alakalmazások helyes működése szempontjából. A változást követően ellenőrizni szükséges a változás eredményét és hatását. A rendszerben bekövetkezett változásokat dokumentáltan kell kezelni illetve a módosításoknak megfelelően a dokumentációkat is frissíteni kell.

### Kártékony kódok elleni védelem

A Hivatal:

1. az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat.
2. frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

…konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

1. rendszeres ellenőrzéseket hajt végre az elektronikus információs rendszeren és végrehajtja a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon a hálózati belépési, vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják;
2. a kártékony kód észlelése esetén blokkolja vagy karanténba helyezi azt; és riassza a rendszeradminisztrátort és az érintett Hivatal által meghatározott további személy(eke)t;
3. ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.
4. Hivatal minden munkaállomásán és szerverén jogtiszta vírusvédelmi rendszert üzemeltet, mely minden, az adathálózatról fogadott illetve oda továbbított adatállományt átvizsgál.
5. A felhasználó rendelkezésére bocsátott informatikai eszközön vírusvédelmi rendszert üzemeltet. A vírusvédelmi rendszert a felhasználónak tilos kikapcsolnia vagy módosítania, illetve tilos módosítani annak beállításait. Abban az esetben, ha a vírusvédelmi rendszer vagy a felhasználó kártékony kódot – pl.: vírust ‑, vagy annak gyanúját észleli, akkor a felhasználó kötelessége azonnal jelenteni az eseményt az adott eszköz üzemeltetési feladataival megbízott rendszergazdának.
6. A felhasználónak tilos a rendelkezésére bocsátott informatikai eszközökön szándékosan kártékony kódokat, illetve Hivatal informatikai biztonsági rendszereinek állapotát bármilyen formában feltérképező szoftvereket tárolni, működtetni, módosítani (mutációkat létrehozni), illetve fejleszteni.
7. A felhasználónak tilos a biztonsági szoftvereket kikapcsolni, működésüket módosítani,

A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell. Felelős: Rendszergazda

### Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

### Az elektronikus információs rendszer felügyelete

A Hivatal:

1. felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
2. azonosítja az elektronikus információs rendszer jogosulatlan használatát;
3. felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
4. védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
5. erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
6. meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

Az elektronikus információs rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, védelme, 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.

Az elektronikus információs rendszer felügyeletének célja, hogy a kibertámadások, vagy a kibertámadásra utaló jelek észlelésre kerüljenek, és feltárásra kerüljön a jogosulatlan lokális, hálózati vagy távoli kapcsolatok és a jogosulatlan használata az elektronikus információs rendszernek.

Automatikus eszközökkel monitorozni kell a tűzfalak, a kiszolgálók, a hálózati aktív eszközök erőforrásait és az azokon futó kritikus szolgáltatásokat.

Az internet kijáratnál behatolás-detektáló rendszert kell működtetni, melynek jelzéseit folyamatosan figyelni kell és meg kell tenni a szükséges reagálásokat.

A fenti feladatok biztosítása a rendszergazda feladata.

### A kimeneti információ kezelése és megőrzése

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

### Biztonsági riasztások és tájékoztatások

Az IBF:

* folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
* folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
* szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;
* a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
* kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel;
* megfelelő ellenintézkedéseket és válaszlépéseket tesz.

## Naplózás és elszámoltathatóság

### Naplózási eljárásrend

Azért, hogy a Hivatal elektronikus információs rendszeréről, rendszerelemeiről naprakész információk álljanak rendelkezésre gondoskodni kell a rendszer naplózási beállításairól. A naplózási beállítások elvégzése a rendszergazda, illetve az adott elektronikus információs rendszer naplózási beállításaihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl. honlap adminisztrátor) feladata és felelőssége.

A Hivatal az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként külön dokumentumban *(Alapkonfiguráció.xlsx - Naplófájlok)* és mellékleteiben határozza meg, az alábbi általános követelmények figyelembevételével:

### Naplózható események

A Hivatal:

1. meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét.
2. egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő Hivatali egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
3. megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.
4. A számon kérhetőség és hibakezelés biztosítása érdekében az informatikai eszközöknek az informatikai rendszer működéséről és különösen az informatikai biztonsági eseményekről helyi naplóállományt generál.
5. A jegyző felelőssége, hogy a kialakított naplózási rendszer a szükséges mértékben biztosítsa a számon kérhetőséget és az auditálhatóságot, tegye lehetővé a bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel azokra, melyek a rendszer biztonságát érintik.
6. Ha a jegyző másként nem rendelkezik az informatikai eszközök minimálisan az alapértelmezett naplózási beállítások szerinti eseményeket naplózza. Az adott informatikai eszköz üzemeltetéséért felelős személy, ha azt az üzemeltetési, üzemeltethetőségi szempontok indokolják saját hatáskörben módosíthatja az alapértelmezett naplóbeállításokat, a jegyző tájékoztatása mellett. A naplóállományokat meghibásodás vagy biztonsági incidens esetén, eseti jelleggel vizsgálja. Meghibásodás esetén a naplóállományok vizsgálata a hibajavításban eljáró üzemeltető feladata. A naplóállományok rendszeres átvizsgálása, a rendszerek naplóállományainak mentése, archiválása alapesetben nem elvárás

A Hivatal az általa üzemeltetett, a felügyelete, irányítása alatt lévő elektronikus információs rendszerk, illetve rendszerelemeik esetében a naplózható, illetve naplózandó biztonsági események körét az alábbiakban határozza meg:

* A rendszergazdai jogosultásggal végzettt tevékenységek köre
* A felhasználók be/ki jelentkezése és profilmódosítások
* Naplósással kapcsolatos események (pl. sikeres/sikertelen)
* Vírusbeállítások módosítása
* Határvédelem, hálózati forgalommal kapcsolatos események logolása
* A rendszerben bekövetkezett hibák, események
* Az adatbázisban történt változások
* A konfigurációkezelésnek és a változáskövetésnek megfelelően a konfigurációs beállítások változása
* Rendszeresemények logolása (pl. leállás, hiba, stb.)

### Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekből gyűjt elegendő információt ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele. (pl. felhasználó azonosítója, esemény időpontja, hibakód, vírustámadás, hálózati cím, port, stb.)

### Időbélyegek

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a Hivatal által meghatározott időmérési pontosságnak. A rendszergazda feladata minden eszközre egységesen megbízható, központi időforrás alkalmazásának konfigurálása.

### A napló információk védelme

Az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. Kizárólag rendszergazdai jogosultsággal rendelkezők férhetnek hozzá a naplóinformációkhoz.

### A naplóbejegyzések megőrzése

A Hivatal a naplóbejegyzéseket meghatározott – a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő – időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében. A naplózási szolgáltatást úgy kell beállítani, hogy lehetőség szerint (figyelembe véve a tárhelyet) legalább 1 évre visszamenőleg rendelkezésre álljanak.

### Naplógenerálás

Az elektronikus információs rendszer:

1. biztosítja a naplóbejegyzés generálási lehetőségét az IBSZ 6.8 pontban meghatározott naplózható eseményekre;
2. lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;
3. naplóbejegyzéseket állít elő az IBSZ 6.8 pont szerinti eseményekre az IBSZ 6.8 pontban meghatározott tartalommal.

Mivel Hivatalban a hivatali gépeket, csak hivatli tevékenységre, munkára lehet használni, így az azokon megvalósuló kommunikáció is csak hivatali lehet. A Hivatal tilt mindenfajta magán kommunikációt a Hivatali rendszerein. Így az e-mailes levelező nem használható nem hivatalos kommunikációra, így az nem tartalmazhat magán információt, adatot. Ennek következtében a Hivatal arra jogosult személyei (Hivatal vezetője, vagy az általa megbízott személy) jogosult az e-malik ellenőrzésére, olvasására. Az ellenőrzésről és annak indokáról a felhasználót tájékoztatjuk.

### Napló ellenőrzés

A rendszergazda köteles a naplóbejegyzések felülvizsgálatát, elemzését a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából legalább havi rendszerességgel elvégezni, s amennyiben problémát tapasztal, akkor az információbiztonsági felelőst tájékoztatni. A Hivatal elektronikus információs rendszereiben a naplók figyelését oly módon kell kialakítani, hogy naplózási hiba esetén küldjön riasztást a rendszert üzemeltető rendszergazdáknak.

## Rendszer- és kommunikációvédelem

### Rendszer- és kommunikációvédelmi eljárásrend

A rendszer- és kommunikációvédelem megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el.

A fentieken túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszer- és kommunikációvédelem érdekében:

### A határok védelme

Az elektronikus információs rendszer:

1. felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;
2. a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a Hivatal belső hálózatától;
3. csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, annak rendszeres frissítéséről kiemelt figyelemmel kell gondoskodni! Felelős: Rendszergazda

### Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem

A Hivatal a szolgáltatás megtagadás alapú támadások elleni védelem érdekében a hálózati, illetve internet szolgáltatást nyújtó szerződéses partnere kiválasztása során előnyben részesíti azon szolgáltatókat, amelyek a hálózati túlterheléses támadások kivédésére saját megoldással, illetve megfelelő kapacitásokkal rendelkeznek.

### Kriptográfiai kulcs előállítása és kezelése

A Hivatal előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

### Kriptográfiai védelem

Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

### Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett Hivatal engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a személyeknek, akik fizikailag jelen vannak az eszköznél. A Hivatal nem használ ilyen infokommunikációs eszközöket.

### Biztonságos név/cím feloldó szolgáltatások

A Hivatal név/cím feloldási szolgáltatást külső, informatikai, illetve telekommunikációs szolgáltató partnertől vesz igénybe.

### Folyamatok elkülönítése

A Hivatal az elektronikus információs rendszereit egymástól elkülönítetten (végrehajtási tartományban tartja) működteti minden végrehajtó folyamatban.

### Záró rendelkezések

Jelen szabályzat 2023.11.10 napján lép hatályba azzal, hogy hatályba léptetésével egyidejűleg a korábban kiadott Informatikai Biztonsági Szabályzat hatályát veszti.

## Módosítások követése

|  |  |
| --- | --- |
| **Módosítások követése:** | **Dátum:** |
| Első változat | 2023-11-10 |

1. sz. melléklet - Felhasználói Nyilatkozat

**Nyilatkozat**

A BALATONFŐKAJÁRI KÖZÖS ÖNKORMÁNYZATI HIVATAL Informatikai Biztonsági Szabályzatának tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

|  |  |  |  |
| --- | --- | --- | --- |
| **Név**  | **Beosztás** | **Dátum**  | **Aláírás** |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |