FEGYVERNEKI POLGÁRMESTERI HIVATAL

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

Jóváhagyom!

dr. Pető Zoltán
Jegyző

Verziószám: 2.1
Dátum: 2026.02.12.

Tartalomjegyzék

1. Az Információbiztonsági Szabályzat

A 7/2024. (VI. 24.) MK rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről a 2024. évi LXIX. törvény, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló, az Európai Parlament és Tanács 2022/2555 irányelv (NIS 2 irányelv) végrehajtásához szükséges egyes rendelkezések alapján a FEGYVERNEKI POLGÁRMESTERI HIVATAL (továbbiakban: Hivatal) információbiztonsági 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 rendszerének belső együttműködését

1.1 A dokumentum célja

Az információbiztonsági 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.

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

1.3 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.

1.4 Alapfogalmak

2022/2555 irányelv alkalmazásában:

1. „hálózati és információs rendszer”:

a) az (EU) 2018/1972 irányelv 2. cikkének 1. pontjában meghatározott elektronikus hírközlő hálózat;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatikus kezelését végzi; vagy

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

2. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

3. „kiberbiztonság”: az (EU) 2019/881 rendelet 2. cikkének 1. pontjában meghatározott kiberbiztonság;

4. „nemzeti kiberbiztonsági stratégia”: valamely tagállam koherens kerete, amely meghatározza a kiberbiztonság területén követendő stratégiai célokat és prioritásokat és a megvalósításukhoz szükséges irányítási intézkedéseket az adott tagállamban;

5. „majdnem bekövetkezett (near miss) esemény”: olyan esemény, amely veszélyeztethette volna a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

6. „esemény”: olyan esemény, amely veszélyezteti a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

7. „nagyszabású kiberbiztonsági esemény”: olyan esemény, amely olyan mértékű zavart okoz, amely meghaladja valamely tagállamnak az arra való reagálása képességét, vagy amely legalább két tagállamra jelentős hatást gyakorol;

8. „eseménykezelés”: minden olyan tevékenység és eljárás, amelynek célja az esemény megelőzése, észlelése, elemzése és elszigetelése vagy az eseményre való reagálás és az eseményt követően a működés helyreállítása;

9. „kockázat”: egy esemény által okozott veszteség vagy zavar lehetősége, amelyet az említett veszteség vagy zavar nagyságrendje és az adott esemény bekövetkezési valószínűsége kombinációjaként kell kifejezni;

10. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

11. „jelentős kiberfenyegetés”: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni kárt okozva súlyos hatást gyakorolhat egy szervezet hálózati és információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

2024. évi LXIX. törvény alkalmazásában

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 információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

3. adatfeldolgozó: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

4. adatkezelés: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

5. adatkezelő: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

6. adatkicserélő szolgáltatás: az elektronikus hírközlésről szóló törvény szerinti fogalom;

7. adatközponti szolgáltatás: olyan szolgáltatás, amely központosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is;

8. adatosztályozás: a szervezet által az elektronikus információs rendszerben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából;

9. ágazaton belüli kiberbiztonsági incidenskezelő központ: olyan kiberbiztonsági incidenskezelő központ, amelyet az e törvény hatálya alá tartozó egy vagy több, egy ágazathoz tartozó szervezet az ágazaton belül meghatározott szakterületen előforduló kiberbiztonsági incidenseinek a központosított és egységes kezelése érdekében üzemeltet;

10. auditor: az e törvény szerinti kiberbiztonsági audittevékenység végzésére jogosult, független gazdálkodó szervezet;

11. behatolásvizsgálat: olyan sérülékenységvizsgálati módszer, amelynek során az IKT-rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárására és kihasználhatóságának ellenőrzésére kerül sor a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával;

12. belső informatikai biztonsági vizsgálat: olyan sérülékenységvizsgálati módszer, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik, vagy a belső hálózatban használt eszköz, vagy rendszerelem vizsgálata kerül végrehajtásra;

13. 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;

14. bizalmi szolgáltatás: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

15. bizalmi szolgáltató: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól

szóló törvény szerinti fogalom;

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

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

18. digitális szolgáltatás: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

19. DNS: hierarchikusan felépülő elnevezési rendszer, más néven doménnévrendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;

20. DNS-szolgáltató: olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja a szervezeten kívüli más szervezet vagy személy részére:

a) autoritatív DNS-szolgáltatás: a doménnév – doménnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű doménnévnyilvántartó szolgáltatás része,

b) rekurzív DNS-szolgáltatás: olyan DNS-szolgáltatás, amely a felhasználók doménnévlekérdezéseit

a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő doménnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére,

c) DNS-gyorsítótárazás: a doménnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt doménnévadatok alapján történő kiszolgálása,

21. doménnév: az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,

22. doménnév-regisztrációt végző szolgáltató: a legfelső szintű doménnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domén regisztrálására;

23. elektronikus hírközlési szolgáltató: az elektronikus hírközlésről szóló törvény szerinti fogalom;

24. elektronikus információs rendszer:

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja,

amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését

végzi, ideértve a kiber-fizikai rendszereket, vagy

c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

25. elektronikus információs rendszer biztonsága: az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

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

27. esemény: az elektronikus információs rendszerben bekövetkezett állapotváltozás;

28. európai kiberbiztonsági tanúsítási rendszer: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti fogalom;

29. felhasználó szervezet: központi rendszert vagy központi szolgáltatást igénybe vevő szervezet;

30. felhőszolgáltatás: olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez;

31. felhőszolgáltató: felhőalapú számítástechnikai szolgáltatást nyújtó szervezet;

32. gyártó: az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója;

33. használatbavétel: az elektronikus információs rendszer adatokkal való feltöltése és rendeltetésszerű használatának megkezdése;

34. honvédelmi célú elektronikus információs rendszer:

a) a honvédelmi szervezetek, a honvédelemért felelős miniszter fenntartói irányítása alá tartozó, honvédségi szervezetnek nem minősülő többcélú szakképző intézmény, a honvédelemért felelős miniszter tulajdonosi joggyakorlása alá tartozó gazdasági Hivatalok, valamint jogszabály szerint a honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági Hivatalok elektronikus információs rendszereinek összessége, amely ágazatspecifikus módon támogatja a honvédelmi ágazaton belüli és ágazatok közötti működést,

b) az ország védelme és biztonsága szempontjából jelentős honvédelmi ágazaton belüli szervezet és infrastruktúra elektronikus információs rendszerei,

c) az ország védelme és biztonsága szempontjából jelentős kettős kijelöléssel nem érintett honvédelmi szervezet és honvédelmi infrastruktúra elektronikus információs rendszerei, valamint

d) a honvédelmi kiberbiztonsági hatóság által alapvető vagy fontos szervezetként azonosított szervezet elektronikus információs rendszere;

35. honvédelmi kiberbiztonsági incidenskezelő központ: a 63. § (2) bekezdése szerint kijelölt szerv;

36. ideiglenes hozzáférhetetlenné tétel: az elektronikus adathoz való hozzáférés ideiglenes megakadályozása;

37. IKT-folyamat: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 14. pontjában meghatározott fogalom;

38. IKT-szolgáltatás: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 13. pontjában meghatározott fogalom;

39. IKT-termék: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 12. pontjában meghatározott fogalom;

40. jelentős kiberbiztonsági incidens:

a) a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,

b) közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely

ba) a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;

bb) súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy

bc) jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;

41. jelentős kiberfenyegetés: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni hátrányt vagy kárt okozva súlyos hatást gyakorolhat egy szervezet elektronikus információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

42. képviselő: Magyarországon letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, Magyarországon nem letelepedett szervezet nevében eljárjon, és akihez vagy amelyhez a kiberbiztonsági hatóság, vagy a kiberbiztonsági incidenskezelő központ az adott szervezet helyett fordulhat;

43. kiberbiztonság: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 1. pontjában meghatározott fogalom;

44. kiberbiztonsági audit: az elektronikus információs rendszerek biztonsági osztályba sorolása, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségének ellenőrzése;

45. kiberbiztonsági hatóság: a 23. § (1) bekezdés a) és b) pontja, valamint (2) bekezdése szerinti hatóság;

46. kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt,továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

47. kiberbiztonsági incidenskezelés: minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;

48. kiberbiztonsági incidenskezelő központ: a 63. § (1) és (2) bekezdése szerinti szerv;

49. kiberbiztonsági incidensközeli helyzet: olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

50. kiberfenyegetés: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 8. pontjában meghatározott fogalom;

51. kiber-fizikai rendszer: olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével;

52. kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató: olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt;

53. kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató: olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról;

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

55. kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének, fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

56. kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és az intézkedések végrehajtása;

57. kockázatmenedzsment keretrendszer: olyan strukturált, ugyanakkor rugalmas megközelítés és szervezeti folyamatok összessége, amely integrálja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén és nyomon követésén keresztül az új és már használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében;

58. közigazgatási szerv: az 1. melléklet 1–13. pontja szerinti szervezet;

59. közösségimédia-szolgáltatási platform: olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással;

60. központi rendszer: egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett elektronikus információs rendszer, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek;

61. központi szolgáltatás: a központi szolgáltató által kötelezően vagy egyedi igény alapján biztosítandó szolgáltatás;

62. központi szolgáltató: olyan szervezet, amely állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújt informatikai és elektronikus hírközlési szolgáltatást;

63. kutatóhely: a tudományos kutatásról, fejlesztésről és innovációról szóló törvény szerinti kutatóhely – az oktatási intézmények kivételével –, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása a kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából;

64. legfelső szintű doménnév-nyilvántartó: olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű doménzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;

65. megfelelőségértékelés: az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek;

66. megfelelőségértékelő szervezet: a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

67. megfelelőségi nyilatkozat: a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

68. megfelelőségi önértékelés: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott

fogalom;

69. mérföldkő: az európai uniós forrásból finanszírozott központi rendszer fejlesztése esetén a Helyreállítási és Rezilienciaépítési Eszköz létrehozásáról szóló, 2021. február 12-i (EU) 2021/241 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja és az Európai Regionális Fejlesztési Alapra, az Európai Szociális Alap Pluszra, a Kohéziós Alapra, az Igazságos Átmenet Alapra és az Európai Tengerügyi, Halászati és Akvakultúra-alapra vonatkozó közös rendelkezések, valamint az előbbiekre és a Menekültügyi, Migrációs és Integrációs Alapra, a Belső Biztonsági Alapra és a határigazgatás és a vízumpolitika pénzügyi támogatására szolgáló eszközre vonatkozó pénzügyi szabályok megállapításáról szóló, 2021. június 24-i (EU) 2021/1060 európai parlamenti és tanácsi rendelet 2. cikk 4. pontja szerinti, valamint a fejlesztésekre irányuló egyéb projektek esetén a projektben meghatározott fogalom;

70. minősített bizalmi szolgáltatás: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

71. minősített bizalmi szolgáltató: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

72. műszaki előírás: az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/ EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet (a továbbiakban: 1025/2012/EU rendelet) 2. cikk 4. pontjában meghatározott fogalom;

73. műveleti célú elektronikus információs rendszer:

a) a rendvédelmi szervek és a nemzetbiztonsági szolgálatok számára törvényben meghatározott

közbiztonsági, nemzetbiztonsági feladatok ellátása érdekében használt elektronikus információs

rendszer és

b) a honvédségi szervezetek által, a törvényben meghatározott katonai műveleti feladatok

– így különösen közvetlen művelettámogatás, -tervezés, -vezetés, helyzetkövetés – ellátása érdekében használt elektronikus információs rendszer;

74. nagyszabású kiberbiztonsági incidens: olyan kiberbiztonsági incidens, amely olyan mértékű zavart okoz, amely

meghaladja Magyarországnak az arra való reagálási képességét, vagy amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol;

75. nem privát felhőszolgáltatás: olyan szolgáltató által nyújtott felhőszolgáltatás, amelyet a szolgáltató bárki számára elérhető módon vagy kizárólag a szervezetek egy meghatározott köre számára nyújt;

76. nemzeti kiberbiztonsági incidenskezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, kiberbiztonsági incidensekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal rendelkezik [európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

77. nemzeti kiberbiztonsági tanúsítási rendszer: IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására, megfelelőségértékelésére Magyarországon alkalmazandó, az európai kiberbiztonsági rendszerek elvei alapján kidolgozott és a tanúsító hatóság által meghatározott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere;

78. nemzeti kiberbiztonsági stratégia: a kiberbiztonság területén követendő stratégiai célokat és prioritásokat, valamint a megvalósításukhoz szükséges irányítási intézkedéseket meghatározó dokumentum;

79. nemzeti kiberbiztonsági tanúsítvány: olyan független harmadik fél által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

80. nemzeti válságkezelési terv: az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti terv, amely meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait;

81. online keresőprogram: az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló, 2019. június 20-i (EU) 2019/1150 európai parlamenti és tanácsi rendelet 2. cikk 5. pontjában meghatározott fogalom;

82. online piactér: olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást használ, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal;

83. regisztrált felhasználói jogosultság: a biztonsági vizsgálatot végző személy számára a sérülékenységvizsgálat elvégzése érdekében célzottan létrehozott felhasználói jogosultság;

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

85. sebezhetőség: IKT-termék, -szolgáltatás, -folyamat gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti az IKT-termék, -szolgáltatás, -folyamat bizalmasságát, sértetlenségét vagy rendelkezésre állását;

86. 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, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

87. sérülékenység: az elektronikus információs rendszer gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti egy elektronikus információs rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását;

88. sérülékenységkezelési terv: a sérülékenységek megszüntetésére irányuló tervdokumentum;

89. sérülékenységvizsgálat: sérülékenységmenedzsment eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontból történő átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre;

90. szabvány: az 1025/2012/EU rendelet 2. cikk 1. pontjában meghatározott fogalom;

91. szervezet: állami szerv vagy állami szervezet, a Polgári Törvénykönyvről szóló törvény szerinti jogi személy, jogi személyiség nélküli szervezet;

92. támogató rendszer: az 1. § (1) bekezdés a)–c) pontja szerinti szervezet alapfeladatainak ellátásában közvetlenül nem részt vevő elektronikus információs rendszer, amely szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el;

93. tanúsítás: független harmadik fél által végzett megfelelőségértékelési tevékenység;

94. tartalomszolgáltató hálózat szolgáltatója: a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója;

95. távoli sérülékenységvizsgálat: olyan sérülékenységvizsgálat, amelynek során

a) az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,

b) automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei,

vagy

c) a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;

96. továbbfejlesztés: az érintett, már működő elektronikus információs rendszer olyan mértékű fejlesztése, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van;

97. üzemeltetési kiberbiztonsági incidens: olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti;

98. üzemeltető: az a természetes személy, jogi személy, jogi személyiség nélküli szervezet vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

99. zárt, teljes körű, folytonos és a kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme,

a) amely az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul,

b) amely az elektronikus információs rendszer valamennyi elemére kiterjed,

c) amely az összes számításba vehető fenyegetést, veszélyt figyelembe veszi, valamint

d) amelynek költségei arányosak a fenyegetések által okozható károk értékével.

1.5 Kapcsolódó szabványok és jogszabályok

- ***ISO/IEC 27001:2022***
  Information technology — Security techniques — Information security management systems — Requirements
- ***NIST SP 800-53 Rev5 2020***
  Security and Privacy Controls for Information Systems and Organizations
- ***GDPR rendelet***
  AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- ***2024. évi LXIX. törvény***
  Magyarország kiberbiztonságáról
- ***418/2024. (XII. 23.) Korm. rendelet***
  Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

- ***7/2024. (VI. 24.) MK rendelet***
  A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

1.6 Szerepkörök

A FEGYVERNEKI POLGÁRMESTERI HIVATAL a részletes hivatali szerepköröket a Szervezeti és Működési Szabályzatban rögzítette.

FEGYVERNEKI POLGÁRMESTERI 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
- biztosítja az egyes elektronikus információs rendszerekre meghatározott biztonsági követelmények teljesülését,
- meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve jóváhagyja és kiadja az Információbiztonsági szabályzatot (jelen Szabályzatot)
- gondoskodik arról, hogy az informatikai szolgáltatás nyújtásához igénybe vett harmadik felek szerződéseiben az Információbiztonsági Szabályzat elvárásai érvényre jussanak
- biztosítja a Hivatal munkatársainak rendszeres időközönkénti biztonságtudatossági oktatását, feladata a képzések tematikájának összeállítása, a képzések végrehajtása.
- intézkedési tervben előírt intézkedések előrehaladásának figyelemmel kísérte
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal
- biztonsági incidensek kivizsgálása
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő mielőbbi és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért
- a kockázatokkal arányosan gondoskodik a feladatkörök szétválasztásáról. (pl. Szoftver fejlesztő, tesztelő. Jogosultság jóváhagyó, beállító. Üzemeltető, műszaki vizsgálatot végző.)
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról

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

Az elektronikus információs rendszer biztonságáért felelős személy (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:

- gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtésében és fenntartásában
- gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről
- előkészíti a Hivatal elektronikus információs rendszereire vonatkozó információbiztonsági szabályzatot,
- előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását,
- előkészíti és a Hivatal vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a szervezet elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat,
- megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal információbiztonsági szabályzatait, szerződéseit,
- folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a Hivatal elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a Hivatal vezetője számára,
- felülvizsgálja, hogy a Hivatal elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és a Hivatal belső szabályozóival,
- az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a Hivatal vezetője számára,
- legalább évente megvizsgálja az intézkedési tervet és beszámolót készít a Hivatal vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket,
- kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal, hatóságokkal, felügyeleti és kormányzati szervekkel, illetve a szakmai szervezetekkel, információbiztonsági szakmai információkkal rendelkező fórumokkal, szervezetekkel, személyekkel
- a Hivatal bármely elektronikus információs rendszerét érintő incidensről tájékoztatja e rendeletben meghatározott szervet,
- felülvizsgálja a Hivatal informatikai biztonsági stratégiáját, szükség esetén aktualizálja azt
- jegyzői kérésre közreműködik az informatikai biztonsági incidensek kivizsgálásában
- kockázatkezelési javaslatok kidolgozása, megvalósulásuk nyomonkövetése
- együttműködik a Kszetv. szerinti kritikus szervezet ellenálló képességéért felelős vezetővel, valamint a Vbö. szerinti ellenálló képességért felelős vezetővel

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 keletkezett valamennyi dokumentumot bekérheti.

Az elektronikus információs rendszer biztonságáért felelős személyt feladata ellátásával kapcsolatosan tudomására jutott adatok és információk tekintetében titoktartási kötelezettség terheli. A titoktartási kötelezettség alól a szervezet vezetője adhat felmentést.

Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó követelményeket, valamint a feladatköröket a **2024. évi LXIX. törvény Magyarország kiberbiztonságáról** 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 üzletmenet 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 a Hivatal számítógépeinek, számítógépes rendszereinek felügyeletét, ezen belül gondoskodik a számítógépek és a kapcsolódó perifériák működőképességéről.
- Közreműködik a Hivatal által használt szoftverek telepítésében, gondoskodik működőképességükről, szükség esetén tanácsaival segíti a szoftverek üzemeltetését végző dolgozók munkáját.
- Felügyeli a Hivatal telekommunikációs rendszereinek (telefon, internet) működését, kapcsolatot tart fenn a telekommunikációs szolgáltatókkal.
- Előkészíti a Hivatal informatikai beruházásait, közreműködik a beszerzett számítástechnikai eszközök rendszerbe állításában, esetenként karbantartási feladatokat lát el az eszközök tekintetében
- Figyelemmel kíséri az internetes információkat (pl. NKI hírlevelek) a lehetséges fenyegetésekről. Szükség esetén módosítja a beállításokat vagy tesz javaslatokat intézkedésre.

Beosztottak, alkalmazottak, munkavállalók: 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 számonkérheti. 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, aktuális híreket és információkat közöl
- A Weboldalra szánt tartalmat előzetesen jóvá kell hagynia a Hivatal vezetőjének

Adatgazda/vagyongazda

- meghatározza az adat/vagyontárgy kezelésére vonatkozó előírásokat,
- dönt a kapcsolódó hozzáférés igényekről,
- szükség esetén javaslatot tesz fejlesztésre.

Kockázatgazda:

- felelős a kockázat kezelés intézkedések meghatározásáért,
- működésének és eredményességének figyelemmel kisérésért
- felelős a kockázat értékelési mutatók és a kockázat nagyságának értékelésért.

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.

1.7 Tevékenységek

FEGYVERNEKI POLGÁRMESTERI HIVATAL meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

1.8 Hivatalrendszer belső együttműködése

FEGYVERNEKI POLGÁRMESTERI HIVATAL belső együttműködését a Szervezeti és Működési Szabályzatban rögzítette.

1.9 Szervezeti szintű alapfeladatok

1.9.1 Információbiztonsági szabályzat

A Hivatal megfogalmazta, dokumentálta, valamint kihirdette az információbiztonsági szabályzatát. Az információbiztonsági szabályzatot a Hivatal, vezetője hagyja jóvá.

Az információbiztonsági szabályzatot 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 súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események bekövetkeztekor, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy a szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése esetén az információbiztonsági szabályzatot újra vizsgálja, szükség szerint módosítja. A Hivatal jelen IBSZ-ben rögzíti az egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

1.9.2 Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevezett ki (külsős alvállalkozó), aki: ellátja a **2024. évi LXIX. törvényben** meghatározott feladatokat. A Hivatal vezetője gondoskodik (alvállalkozó esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően.

1.9.3 Intézkedési terv és mérföldkövei

A Hivatal vezetése intézkedési tervet készít az EIR-ben tervezett korrekciós intézkedések dokumentálására, hogy a védelmi intézkedések értékelése során feltárt gyengeségeket vagy hiányosságokat kijavítsák, valamint a rendszer ismert sérülékenységeit csökkentsék vagy megszüntessék. Az így elkészített intézkedési tervet és a mérföldköveket, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit legalább évente felülvizsgálja és karbantartja.

1.9.4 Kockázatok kezelése

Az elektronikus információs rendszer 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 kidolgozásra. 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 rendszer 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 sorolás fejezetben leírtak szerint elvégezze a besorolást.

1.9.5 Biztonsági osztályba sorolás

Az elektronikus információs rendszerek, valamint az azokban kezelt adatok költséghatékony védelmének biztosítása érdekében a Hivatal a vonatkozó jogszabályokban leírtak szerint be sorolja az elektronikus információs rendszereket egy-egy biztonsági osztályba a kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kockázata alapján.

A szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet a szervezet vezetője hagy jóvá, hatáselemzés alapján kell elvégezni. Az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság ajánlásként hatáselemzési módszertanokat ad ki. Ha a szervezet saját hatáselemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.

A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a szervezet felelőssége.

- Az **„alap”** biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel:
- az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,
- a szervezet üzleti vagy ügymenete szempontjából csekély értékű vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,
- a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy
- a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.
- A **„jelentős”** biztonsági osztály esetében közepes káresemény következhet be, mivel:
  nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,
  személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),
  a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,
- a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.
- A **„magas”** biztonsági osztály esetében nagy káresemény következhet be, mivel különleges személyes adat nagy mennyiségben sérülhet,
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
- nemzeti adatvagyon helyreállíthatatlanul megsérülhet,

- az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,
- a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,
- súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy
- a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

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 hatóság által 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 jelen szabályzatban rögzítse, és a jegyző számára előterjessze, aki gondoskodik a módosított szabályzat érvénybe léptetéséről.

1.9.6 Végrehajtás gyakorisága

A biztonsági osztályba sorolást legalább kétévenként vagy az elektronikus rendszer biztonságát érintő, jogszabályban meghatározott változás 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.

2 Rendszerek besorolási nyilatkozata

2024. évi LXIX. törvény hatálya alá tartozó elektronikus információs rendszert a **Magyarország kiberbiztonságáról** szerinti érintett szervezet (a továbbiakban: érintett szervezet) a **7/2024. (VI. 24.) MK rendelet** 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.

A szervezet elektronikus információs rendszerei, valamint az azokban kezelt adatok, a nyújtott szolgáltatások kockázatokkal arányos védelmének biztosítása érdekében a szervezet az e törvény hatálya alá tartozó elektronikus információs rendszereit „alap", „jelentős" vagy „magas" biztonsági osztályba sorolja az érintett elektronikus információs rendszer sértetlensége és rendelkezésre állása, valamint az általa kezelt adat bizalmassága, sértetlensége és rendelkezésre állásának kockázata alapján, szigorodó védelmi előírásokkal.

A biztonsági osztályba sorolást a szervezet vezetője határozza meg, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolás eredményét a szervezet az elektronikus információs rendszerek nyilvántartásában rögzíti.

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 Információbiztonsági 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 ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

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.

FEGYVERNEKI POLGÁRMESTERI HIVATAL nyilatkozatban rögzíti, hogy a 2026. 02 hó időszakban, a Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával egy kockázatértékelés során végzett *7/2024. (VI. 24.) MK* rendeletnek való megfelelés alapján végzett vizsgálatának eredményeként a Hivatal rendszereinek biztonsági osztályai a következők:

Sorszám:	A rendszer megnevezése:	Bizalmasság	Sértetlenség	Rendelkezésre állás	Biztonsági osztály
1.	IT helyi infrastruktúra	X	X	X	**Alap**
2.	fegyvernek.hu	X	X	X	**Alap**

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

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

3 Intézkedési terv és mérföldkövei

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

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

frissíti a meglévő intézkedési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések, a független auditok és felülvizsgálatok, valamint a folyamatos felügyelet eredményei alapján.

A jegyző felelőssége biztosítani az elektronikus információs rendszerek biztonságáért felelős személy szakmai támogatása mellett az intézkedési 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 az intézkedési terv feladatainak előrehaladásában az intézkedési terv végrehajtását veszélyeztető probléma jelentkezik, akkor a jegyző feladata rendelkezni a probléma kezelésének módjáról, szükség esetén az intézkedési terv átütemezéséről.

3.1 Az elektronikus információs rendszerek nyilvántartása

Az jegyző felelőssége, hogy a Hivatal teljeskörű, naprakész nyilvántartást vezessen a Hivatalban használt elektronikus információs rendszerekről. Minden rendszerre nézve egy elektronikus nyilvántartást vezet, melyet szükség szerint aktualizál (pl.: új rendszer bevezetése, meglévő rendszer kivezetése). A nyilvántartás tartalmazza:

a) a rendszer által támogatandó üzleti célokat, funkciókat és folyamatokat
b) a tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyeket vagy szervezeteket,
c) az érintett vagyonelemeket,
d) a rendszer szervezeti és technológiai határát,
e) a rendszer által feldolgozandó, tárolandó és továbbítandó adatköröket és azok életciklusát,
f) a rendszerrel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését
g) a rendszer helyét a szervezeti architektúrában, amennyiben a szervezet rendelkezik vele;

A Hivatal az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(*EIR nyilvantartas*)* kezeli. A rendszergazda feladata a nyilvántartás elkészítése és az évente történő felülvizsgálata.

3.2 A biztonsági teljesítmény mérése

A Hivatal kialakította a megfelelő működés az elért eredmények, teljesítmények figyelemmel kísérésének módszereit, melyet beépített folyamataiba, szabályozásaiba.

A biztonság szintjének értékelésére, figyelemmel kísérésére információbiztonsági teljesítmény/eredményesség mutatókat, és célértékeket határoz meg. A döntésekről feljegyzéseket őriz meg a **rendszergazda**. Az ő feladata a terv megvalósulásának követése, a teljesítmény és eredményesség mutatók figyelése, és erről a **vezetőség** tájékoztatása. A szervezet a kockázatokat minden változáskor, de legalább évente felülvizsgálja. A felülvizsgálat eredményei alapján az első felméréshez hasonlóan a **vezetőség** hozza meg a döntéseket.

Az IBIR működésének operatív figyelemmel kíséréséért a rendszergazda a felelős, melynek során többek között figyelemmel kíséri az intézkedési és a ***kockázatjavítási tervek, információbiztonsági célok*** megvalósulását, a ***teljesítmény és eredményesség mutatók*** alakulását, a biztonsági ellenőrzések tapasztalatait, a feltárt gyengeségeket, incidenseket és kezelésüket, a külső, belső környezeti változásokat, melyek hatással lehetnek az IBIR működésére, eredményességére.

Az IBIR eredményességét, működését, a szabályozások, intézkedések alkalmasságát, betartását a szervezet belső auditok keretében is ellenőrizi.

A mérések végrehajtásában az rendszergazda, a Hivatal munkatársai, valamint a Társassággal 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.

A vezetőség legalább évente áttekinti az IBIR működését, és dönt a szükséges intézkedésekről, fejlesztésekről. A tervezett változásokat megtervezzük melyek alapján gondoskodunk, hogy folyamatosan fenntartsuk az IBIR megfelelő működését.

A FEGYVERNEKI POLGÁRMESTERI HIVATAL folyamatosan fejleszti információbiztonsági rendszerét, figyelembe véve a működési tapasztalatokat, külső és belső jelzéseket, környezeti változásokat, érdekelt felek elvárásainak változását, a célokat, hogy folyamatosan megfeleljen a követelményeknek. A fejlesztésekhez kapcsolódóan aktualizálja dokumentációs rendszerét is.

3.3 Szervezeti architektúra

A Hivatal kifejleszti és fenntartja a Hivatali szervezetrendszert, amely tekintettel van mindazon kockázatokra, amelyek hatással lehetnek a szervezeti működésre, az eszközökre, az egyénekre és más szervezetekre.

3.4 A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

A Hivatal működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket.

4 Hozzáférés felügyelet

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.

A felülvizsgálat évente esedékes, valamint súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése esetén.

4.1 Felhasználói fiókok kezelése

A Hivatal:

a) Meghatározza és dokumentálja a rendszerben engedélyezett és kifejezetten tiltott fióktípusokat;
b) kijelöli a felhasználói fiókok fiókkezelőit;
c) kialakítja a csoport- és szerepkör tagsági feltételeket és kritériumokat;
d) meghatározza a rendszerben engedélyezett felhasználókat, a csoport- és szerepkör tagságokat A hozzáférési jogosultságokat és a felhasználói fiókokhoz tartozó szükséges jellemzőket minden egyes felhasználói fiókra
e) A meghatározott szerepköröket betöltő személyek jóváhagyását kéri a felhasználói fiókok létrehozására vonatkozó kérelmek esetén.
f) Létrehozza, engedélyezi, módosítja, letiltja és törli a fiókokat a meghatározott irányelvek, eljárások, előfeltételek és kritériumok alapján
g) Nyomon követi a fiókok használatát
h) értesíti a fiókkezelőket és a meghatározott személyeket vagy szerepköröket a következő esetekben, ha:
    - a felhasználói fiókokra már nincsen szükség;
    - a felhasználók kiléptek vagy áthelyezésre kerültek;
    - az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;
i) Engedélyezi a rendszerhez való hozzáférést a következők alapján:
    - az érvényes hozzáférési engedély,
    - a tervezett rendszerhasználat,
    - egyéb, a szervezet által meghatározott jellemzők;

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. Összehangolja a fiókkezelési folyamatokat a felhasználók jogviszonyának megszűntetési folyamataival.

4.2 Hozzáférés ellenőrzés érvényesítése

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

4.3 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.

4.4 Privilegizált fiókok

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

4.5 Sikertelen bejelentkezési kísérletek

Az elektronikus információs rendszerek szintjén és a hálózati eszközök szintjén is ki kell kényszeríteni a következő fiókzárolási házirendet:

3 egymást követő sikertelen bejelentkezési kísérlet esetére 30 percre zárolni kell a fiókot és a számlálót 30 perc után nullázni kell. Ahol a számláló nullázása nem valósítható meg, ott zárolni kell a felhasználói fiókot és csak a rendszergazda oldhatja fel a zárolást.

4.6 A rendszerhasználat jelzése

Az EIR a rendszer használata előtt megjelenít a felhasználóknak egy meghatározott rendszerhasználati értesítést vagy üzenetet, amely biztonsági értesítést tartalmaz a szervezetre vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint és tartalmazza, hogy:

- A felhasználók a szervezet EIR-ét használják.
- A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.
- A rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.
- A rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti.
- Az EIR mindaddig fenntartja a rendszerhasználati értesítést a képernyőn, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket a rendszerbe való bejelentkezésre vagy a rendszerhez való további hozzáférésre.

Nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza:

- A felhasználók a szervezet EIR-ét használják.
- A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.
- A rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.

4.7 Munkaszakasz zárolása

A rendszergazdának meghatározott időtartamú (pl.: 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.

4.8 Képernyőtakarás

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

4.9 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.

4.10 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

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

4.11 Távoli hozzáférés

A távoli elérés VPN kapcsolaton keresztül engedélyezett. Kizárólag olyan munkaállomás vagy laptop használható távoli munkavégzésre mely naprakész (az operációs rendszer és az alkalmazások biztonsági frissítései telepítésre kerültek), bekapcsolt tűzfallal, vírusvédelemmel rendelkezik.

4.12 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

4.13 Mobil eszközök hozzáférés ellenőrzése

A Hivatal:

- Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszközök számára, beleértve azokat az

eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el.
- engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

Konfigurációs követelmények, kapcsolódási követelmények és alkalmazási útmutató

- **Eszközbiztonság:**
    - Eszköz zárolása jelszóval, PIN-kóddal vagy biometrikus azonosítással.
    - Titkosítás használata az eszközön tárolt adatok védelmére.
    - Operációs rendszer és alkalmazások naprakészen tartása.
    - Automatikus frissítések engedélyezése.
    - Automatikus zárolás 10 perc után
    - Csak ellenőrzött, engedélyezett alkalmazások telepítése.
- **Hálózati hozzáférés:**
    - VPN használata a szervezet hálózatához való biztonságos kapcsolódáshoz, különösen, ha az eszköz a szervezeti területen kívül van.
    - Amennyiben lehetséges kétfaktoros azonosítás (2FA) használata minden bejelentkezéshez
- **Adatátvitel:**
    - Csak titkosított csatornák használata (pl. HTTPS, SSL/TLS).
- **Felhasználói képzés:**
    - Jelentési folyamat az elveszett vagy ellopott eszközök esetén.
    - Távoli munkavégzés szabályai, például nyilvános Wi-Fi hálózatok kerülése vagy VPN kötelező használata.
- **Hozzáférés jóváhagyása:**
    - Csak a biztonsági követelményeknek megfelelő eszközök kapnak engedélyt a szervezeti rendszerek elérésére.
    - Engedélyezési kérelem jóváhagyása a rendszergazda által.
- **Folyamatos ellenőrzés:**
    - Eszközök rendszeres biztonsági állapotának ellenőrzése.
    - Gyanús tevékenységek esetén hozzáférés automatikus tiltása.

Hozzáférés korlátozása:

- A mobil eszközök csak az adott felhasználó számára releváns rendszerekhez és alkalmazásokhoz férhetnek hozzá.
- Hozzáférési engedély visszavonása inaktivitás vagy szabálysértés esetén.

4.14 Külső elektronikus információs rendszerek használata

A Hivatal és a külső rendszer működtetője meghatározza, hogy:

a) milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;
b) külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Hivatal által ellenőrzött információkat.
c) külső szolgáltató a Hivatali rendszeren, azonosítatlan és engedéllyel nem rendelkező tevékenységet nem végezhet.
d) megtiltja a meghatározott típusú külső rendszerek használatát.

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.)

4.15 Nyilvánosan elérhető tartalom

A Hivatal:

a) Kijelöli azokat a személyeket, akik jogosultak arra, hogy információkat tegyenek nyilvánosan hozzáférhetővé;
b) Képzést biztosít a jogosult személyek számára, hogy biztosítsa, hogy a nyilvánosan hozzáférhető információk nem tartalmaznak nem nyilvános információkat.
c) Áttekinti az információ tervezett tartalmát a nyilvánosan hozzáférhető rendszerbe történő közzététel előtt, annak érdekében, hogy biztosítsa, hogy nem tartalmaznak nem nyilvános információkat.
d) Meghatározott gyakorisággal áttekinti a nyilvánosan hozzáférhető rendszer tartalmát a nem nyilvános információk szempontjából, és eltávolítja az ilyen információkat, ha felfedezik őket.
e) A Hivatal nyilvánosan elérhető rendszerként definiálja például a Hivatal publikus weboldalát.
f) A publikus felületeken való közzétételt és a médiával való kommunikációt a jegyző szabályozza, a Hivatal külső kommunikációjáért a jegyző a felelős.
g) A Hivatali honlap tartalommenedzsmentjét a rendszergazda vagy a jegyző által megbízott személy végzi.
h) 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 honlapot.

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.

5 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:

a) felelős a képzési kritériumok meghatározásáért
b) biztosítja a képzéshez a szükséges erőforrásokat
c) gondoskodik a képzések fontosságának tudatosításáról a teljes szervezetben

Az IBF:

a) felelős a képzési rendszer kialakításáért, fenntartásáért
b) felelős a szükséges oktatások megtartásáért, megtartatásáért

A munkatársak:

a) felelősek a képzési előírások betartásáért, a képzések során leadott anyagok elsajátításáért

5.1 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 információbiztonsági 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.
- felhívjuk a figyelmet belső fenyegetések potenciális jeleinek felismerésére és jelentésére.
- 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.

5.2 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 információbiztonsági szabályok megismeréséhez és megértéséhez szükséges minden szükséges támogatást.

5.3 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.

5.4 Képzési eljárásrend

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.

6 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.

Felülvizsgálat évente esedékes, illetve súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése esetén.

6.1 Naplózható események

A Hivatal:

a) meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét.
b) Egyezteti a naplózási elvárásokat a naplózási információt igénylő szervezeti egységekkel, hogy iránymutatással és információkkal segítse a naplózandó események kiválasztását.
c) Meghatározza az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket.
d) Indokolja, hogy a kiválasztott eseménytípusok, miért alkalmasak a biztonsági események utólagos kivizsgálásának támogatására;
e) Meghatározott gyakorisággal felülvizsgálja és frissíti a naplózásra kiválasztott eseménytípusokat.
a) 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.
b) 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 Hivatal az általa üzemeltetett, a felügyelete, irányítása alatt lévő elektronikus információs rendszerek, illetve rendszerelemeik esetében a naplózható, illetve naplózandó biztonsági események körét az alábbiakban határozza meg:

- A rendszergazdai jogosultsággal végzett 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.)

6.2 Naplóbejegyzések tartalma

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

6.3 Naplózás tárkapacitása

A Hivatal elegendő méretű tárkapacitást biztosít a naplózásra, figyelembe véve a naplózási funkciókat és a meghatározott megőrzési követelményeket.

6.4 Naplózási hiba kezelése

A Hivatal naplózási hiba esetén:

- Riasztja a meghatározott személyeket vagy szerepköröket a szervezet által meghatározott időn belül (közel valós időben).
- További meghatározott intézkedéseket hajt végre.

6.5 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.

6.6 Időbélyegek

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben amelyek megfelelnek a szervezet által meghatározott pontosságra vonatkozó követelményeknek, a koordinált világidőt használják és magukba foglalják a helyi időeltolódást. A rendszergazda feladata minden eszközre egységesen megbízható, központi időforrás alkalmazásának konfigurálása.

6.7 A napló információk védelme

Az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor értesíti a meghatározott személyeket vagy szerepköröket. Kizárólag rendszergazdai jogosultsággal rendelkezők férhetnek hozzá a naplóinformációkhoz.

6.8 Naplógenerálás

Az elektronikus információs rendszer:

a) Biztosítja a naplóbejegyzés generálási képességet a "Naplózható események" pontban meghatározott naplózható eseményekre.;
b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;
c) Naplóbejegyzéseket állít elő a "Naplózható események" pont szerinti eseményekre az "Naplóbejegyzések tartalma" pontban meghatározott tartalommal.

6.9 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.

7 Biztonsági értékelések

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

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

7.1 Biztonsági értékelések – Kiberbiztonsági audit

A Hivatal független auditorokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.

7.2 Információcsere

A Hivatal jóváhagyja és szabályozza az információcserét az EIR és más rendszerek között, összhangban a kapcsolódásokra és az információcserére vonatkozó biztonsági megállapodásokkal, továbbá figyelembe veszi a szolgáltatási szintre, a felhasználókra és a titoktartásra vonatkozó, valamint a szervezet által meghatározott egyéb megállapodásokat.

Minden egyes információcsere-megállapodás keretében dokumentálja az egyes rendszerek interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét, valamint rögzíti a megosztott információk hatásának szintjét is.

Rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat.

7.3 Engedélyezés

A Hivatal:

- Kijelöl egy engedélyezésért felelős személyt, aki az EIR-ért felel.
- Kijelöl egy felelős személyt, aki a szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel.
- Biztosítja, hogy az engedélyezésért felelős személy az EIR használatbavételét megelőzően:
    - elfogadja a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását; és. a szervezet vezetőjével engedélyezteti a rendszer működését.
    - Biztosítja, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát.
    - Rendszeresen felülvizsgálja az engedélyeket.

Az engedélyezésért felelős személy a rendszergazda szorosan együttműködve az IBF-el.

7.4 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.

7.5 Folyamatos felügyelet – Kockázatmonitorozás

A Hivatal biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza:

- a hatékonyság ellenőrzését;
- a megfelelés ellenőrzését; és
- a változások nyomon követését.

7.6 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 elektronikus információk típusát.

Az összekapcsolást az 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.

7.7 Belső rendszerkapcsolatok

A Hivatal belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását;

A Hivatal elektronikus információs rendszere több elemből épül fel, melyek bizonyos interfészeken 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

8 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.

8.1 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 elektronikus 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.

8.2 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 elektronikus 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.

Fizikai hozzáférési korlátozások:

- Csak az **engedélyezett rendszergazdák** léphetnek be a szerverterembe, férhetnek hozzá a rack szekrényhez
- A belépéseket és tartózkodásokat **beléptetési napló** rögzíti.
- Harmadik fél (karbantartó, beszállító) csak előzetesen jóváhagyott, **kísért hozzáféréssel** léphet be.
- A hálózati eszközök és szerverek fizikai portjain a hozzáférést lezárt rackek és portzárak biztosítják.

Logikai hozzáférési korlátozások:

- Csak változáskezelésben jóváhagyott, szerepkör-alapú hozzáféréssel rendelkező személyek módosíthatják a konfigurációt. (Rendszergazda)
- Az admin jogosultságok névre szólóak, nem megosztottak.
- A kritikus rendszereken a konfiguráció módosításához jóváhagyott munkalap (Change Request) szükséges.

Éles rendszerekhez való hozzáférés időben korlátozott („just-in-time access”).

8.3 Előzetes tesztelés és megerősítés

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő elektronikus 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.

8.4 Biztonsági hatásvizsgálat

A változtatás megkezdése előtt a rendszergazdának 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.

8.5 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.

8.6 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.
- A leltár pontosan tükrözi az EIR-t.
- leltár tartalmazza a rendszeren belül található összes elemet.

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

8.7 A szoftverhasználat korlátozásai

A Hivatal:

a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;
b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
c) ellenőrzi és dokumentálja az állománymegosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett művek jogosulatlan terjesztésére, megjelenítésére, előadására vagy sokszorosítására.
d) 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!
e) 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.
f) 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.
g) 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.
h) 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.
i) Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből.

8.8 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 telepítésére, módosítására.

9 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:

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

9.1 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:

a) meghatározza az alapfeladatokat (a biztosítandó szolgáltatásokat és azok elvárt szolgáltatási szintjét [angolul SLA]) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
b) tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat;
c) kjelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeke és azok elérhetőségét;
d) meghatározza az EIR összeomlása, kompromittálódása vagy hibája ellenére is biztosítandó szolgáltatásokat;
e) tartalmazza az EIR végleges, teljeskörű helyreállításának tervét, mely garantálja, hogy az eredetileg tervezett és megvalósított védelmi intézkedések a helyreállítás után ne sérüljenek;
f) szabályozza az üzletmenet-folytonossági információk megosztását; és
g) szervezet által meghatározott személyek vagy szerepkörök által felülvizsgált és jóváhagyott.
h) Megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint A szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az EIR-ekre vonatkozó üzletmenet-folytonossági tervet.

i) összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
j) meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
k) 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;
l) tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, személyeket és Hivatali egységeket;
m) Az üzletmenet-folytonossági terv tesztelése, gyakorlata vagy tényleges alkalmazása során levont tanulságokat beépíti a tesztelési és gyakorlati folyamatokba
n) gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
o) összhangban áll az Informatikai Biztonságpolitikával, valamint igazodik a szervezet felépítéséhez és architektúrájához;
p) fenntartja a Hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;

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 biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése, új szolgáltatás, üzleti folyamat bevezetése, 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 hozzáféréstől.

9.2 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 az 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)

9.3 Infokommunikációs szolgáltatások

A Hivatal 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.

9.4 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.

9.5 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 politikája részének.

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

Feladatok és felelősségek

A mentések szakszerű elvégzését a rendszergazda, vagy a Hivatallal kötött megállapodásban rögzítettek szerint az adott elektronikus információs rendszer üzemeltetője 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.

9.6 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.

10 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.

A felülvizsgálat évente esedékes, valamint súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése esetén.

10.1 Azonosító kezelés

A Hivatal:

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

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

10.2 A hitelesítésre szolgáló eszközök kezelése

A Hivatal vezetése által kijelölt személy:

a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
c) biztosítja, hogy a hitelesítő eszközök a tervezett felhasználáshoz megfelelő erősségű mechanizmussal rendelkezzenek.;
d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az első használat előtt;
f) gondoskodik a hitelesítő eszközök tartalmának megváltoztatásáról vagy frissítéséről meghatározott gyakorisággal, vagy amikor meghatározott események bekövetkeznek.

g) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
h) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
i) Megváltoztatja a csoporthoz vagy szerepkörhöz rendelt fiókok hitelesítő eszközeinek tartalmát, amikor a fiókokhoz tartozó tagok közül valaki eltávolításra kerül.

10.3 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;

- A Hivatal fenntartja a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját, és ezt a listát a szervezet által meghatározott gyakorisággal frissíti, továbbá minden olyan esetben, amikor a szervezeti jelszavakat közvetlenül vagy közvetett módon veszélyeztetik.
- Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján.
- A jelszavakat csak kriptográfiailag védett csatornákon keresztül továbbítja.
- Megköveteli a jelszó azonnali megváltoztatását fiókvisszaállítás esetén.
- Engedélyezi a felhasználóknak hosszú jelszavak és jelmondatok kiválasztását, beleértve a szóközöket és a nyomtatható karaktereket.
- Automatizált eszközökkel támogatja a felhasználókat az erős jelszavak kiválasztásában.
- A jelszavakra a szervezet által meghatározott összetételi és komplexitási szabályokat érvényesíti.

10.4 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.

10.5 Hitelesítési információk visszajelzésének elrejtése

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

10.6 Hitelesítés kriptográfiai modul esetén

Az EIR olyan mechanizmusokat alkalmaz a kriptográfiai modul hitelesítéséhez, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának, a hatályos törvényeknek, a végrehajtási utasításoknak, szabályzatoknak, szabványoknak.

10.7 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett Hivatalon kívüli felhasználókat és tevékenységüket valamint a nevükben futó folyamatokat.

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.

10.8 Újrahitelesítés

A Hivatal meghatározott körülmények vagy helyzetek esetén megköveteli a felhasználótól az

újrahitelesítést.

11 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, rendelkezésre 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.

11.1 A biztonsági események kezelése

Az elektronikus 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, terjedelemét, az általuk okozott károkat, helyreállítás lehetőségeit és költségeit, a helyreállítás időtartamát.

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

11.2 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.

11.3 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 bejelentést a rendszergazda e-mail címre kell megtenni amennyiben ez nem

lehetséges akkor telefonon vagy személyesen. 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 haladéktalanul jelenti az elektronikus információs rendszerekben bekövetkezett, illetve a tudomásukra jutott fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is – a nemzeti kiberbiztonsági incidenskezelő központ részére a rendeletben meghatározottak szerint.

Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni (dokumentálás, eljárások, ellenőrzés, utóvizsgálat stb.) 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.

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.

11.4 Biztonsági események kategorizálása

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

- enyhe biztonsági esemény
- súlyos biztonsági esemény

<u>Enyhe biztonsági esemény</u>

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.

<u>Súlyos biztonsági esemény:</u>

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.

11.5 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.

11.6 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
    a. Incidensek okának azonosítása, elemzése, kivizsgálása
    b. Bizonyítékok begyűjtése
    c. Incidens behatárolása
    d. 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

3. Elszigetelés (az esemény jellegéből adódóan)
4. Megszüntetés

a. A szükséges intézkedések meghatározása
b. 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

5. Helyreállítás

Helyreállítási felelősök kijelölése:

a. Az Üzletmenet-folytonosságot érintő események esetén (az esemény jellegéből adódóan) az Üzletmenet-folytonossági tervben rögzített módon kell eljárni.
b. 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 az 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 az Jegyző számára történő megküldése.

11.7 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.

12 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. Az eljárásrendet és a szabályzatot a karbantartásért felelős szerepköröket érintő szervezeti változások, a használat vagy a szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése, karbantartási szerződések módosulása, karbantartási hiányosságból adódó biztonsági incidens esetén felül kell vizsgálni, aktualizáni kell.

12.1 Rendszeres karbantartás

A Hivatal által megbízott személyek vagy vállalkozók:

a) a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról, cserékről készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és hogy a rendszert vagy a rendszerelemeket a helyszínen szervizelik-e, vagy más helyszínre szállítják.
c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;

d) az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
f) 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;
g) számítógépek esetében, ha a javítás külső helyszínen történik, az esetleges adattartalmat töröljük, az el- és visszaszállítást pedig dokumentáljuk
h) a nem javítható eszközöket a leírtaknak megfelelően selejtezzük, esetleges adattartalmukat pedig – szükség esetén véglegesen és helyreállíthatatlanul – töröljük
i) a tervezett karbantartások mértéke és gyakorisága megfelel a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer elvégzésre kerül;
j) minél nagyobb mértékben járuljon hozzá a kockázatok (a működési szabályok betartásával) csökkentéséhez, a helyes és rendszeres karbantartottság révén;

12.2 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 a rendszergazda őrzi.

12.3 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 végezhetik 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.

12.4 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.

12.5 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 információbiztonsági szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;
- erős hitelesítési eljárásokat 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.

12.6 Karbantartó személyek

A Hivatal kialakít egy folyamatot a karbantartási munkákhoz szükséges hozzáférési jogosultságok kezelésére, és nyilvántartást vezet a hozzáférési jogosultsággal rendelkező karbantartó szervezetekről vagy személyekről.

Ellenőrzi az EIR-en kíséret nélkül karbantartást végző személyek hozzáférési jogosultságait.

Kijelöli a szervezethez tartozó és a kívánt hozzáférési jogosultságokkal, valamint a megfelelő műszaki szakértelemmel rendelkező személyeket arra, hogy felügyeljék a szükséges jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

13 Adathordozók védelmére vonatkozó eljárásrend

A Hivatal jelen eljárásrendjében rögzíti az adathordozók védelmére vonatkozó előírásait.

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

a) hozzájárul az adathordozók kezeléséből eredő kockázatok csökkentéséhez;
b) 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.

A szabályzatot és az eljárásrendet felül kell vizsgálni és aktualizálni kell abban az esetben is amennyiben a használt adathordozók terén történt jelentős változás, az adathordozók védelmi megoldásaiban történt jelentős változás, új EIR-ek bevezetése, adathordozók nem megfelelő védelméből adódó biztonsági incidens következik be.

13.1 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.

13.2 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.

13.3 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.

13.4 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.

13.5 Adathordozók törlése

A meghibásodott, további felhasználásra alkalmatlan adathordozókat a rendszergazda 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.

13.6 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 információbiztonsági 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.

14 Fizikai Védelmi Intézkedések

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. Az eljárásrendet felül kell vizsgálni és aktualizálni kell telephely, adatközpont változások, új technológia a fizikai védelemben, új szerződések a fizikai védelmet ellátó szervezettel kapcsolatban, rendkívüli fizikai biztonsági esemény esetén.

14.1 Fizikai belépési engedélyek

A Hivatal:

a) összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
b) belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
c) rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
d) eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
e) 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 jogosultságokat 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
0. 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 elektonikus információs rendszerek (pl. tárgyalók) így ide a Hivatal minden munkatársa beléphet, illetve a látogatók, ügyfelek is kíséret és felügyelet mellett.
2. biztonsági zóna	Magas	A Hivatal feladatait támogató elektronikus információs rendszereinek helyt adó helyiségek A belépés csak az arra jogosultak számára lehetséges, a látogatók, ügyfelek, belépése és ott tartózkodása csak kíséret és felügyelet mellett engedélyezett.
3. biztonsági zóna	Kritikus	IT és ellátó infrastruktúra valamennyi helyisége pl. szerverhelyiség (ideértve a szerverfunkciójú számítógépeket, adatmentő szervereket is, hálózati eszközöket). A belépés kizárólag a rendszergazdának engedélyezett. Munkatársak, ügyfelek, látogatók, karbantartók, stb. kizárólag felügyelettel léphetnek be és tartózkodhatnak ott.

14.2 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 személy/személyzet nem takaríthat felügyelet nélkül az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben. (pl. szerverszoba)

A Hivatal:

a) kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
b) ellenőrzi az egyéni jogosultságokat a létesítménybe való belépés előtt;

c) ellenőrzi a létesítménybe való be- és kilépést a meghatározott fizikai beléptető rendszerek vagy eszközök illetve őrök segítségével;
d) naplózza a fizikai be- illetve kilépéseket;
a) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
b) gondoskodik a kíséretről a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
c) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést biztosító eszközöket;
d) nyilvántartást vezet a fizikai belépést ellenőrző eszközökről és meghatározott gyakorisággal frissíti azt;
e) a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;
f) 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;
g) 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 regisztrációjára szolgáló naplót a „Szerverszoba belépési nyilvántartás" tartalmazza. A hozzáférési naplókat legalább 90 naponta felül kell vizsgálni. A felülvizsgálatot abban az esetben is el kell végezni, ha adott időn (egy napon) belül túl sok egyforma belépési kísérlet, munkaidőn túli belépési kísérletek, rendkívüli események (betörés, beléptető rendszer áramellátását, működését megszakító események) történtek. A belépési naplókat legalább 1 évig meg kell őrizni. A látogatói belépési nyilvántartás rendellenességeit a rendszergazda jelenti az IBF-nek.

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)

14.3 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;
- 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.

14.4 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.

14.5 Vészvilágítás

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

14.6 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.

14.7 Hőmérséklet és páratartalom ellenőrzés

A szerverhelyiségben elhelyezett központi kiszolgáló egységek biztonságos működése érdekében a hőmérsékletet 18-28 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 vezetni 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

14.8 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) 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.

14.9 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, munkatárs, 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.

14.10 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.

14.11 A kiemeneti eszközök hozzáférés ellenőrzése

A fénymásoló és nyomtató berendezéseket/multifunkciós eszközöket és minden egyéb kimeneti eszközt védett területen belül kell elhelyezni, ahol a felügyeletük biztosítható, illetve az illetéktelen hozzáférés megakadályozható. A kinyomtatott vagy másolt dokumentumokat 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.

15 Tervezés

A Hivatal:

Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságtervezési szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal a biztonságtervezési eljárásrendet, amely a biztonságtervezési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonságtervezési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. (IBF)

Felülvizsgálja és frissíti az aktuális biztonságtervezési szabályzatot és a biztonságtervezési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal (évente) és a szervezet által meghatározott események bekövetkezését követően.

A biztonságtervezési szabályzat, eljárásrendet felül kell vizsgálni és aktualizálni kell a súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy a szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése esetén.

A biztonságtervezési szabályzat, eljárásrend felülvizsgálatának és frissítésének gyakorisága évente esedékes.

15.1 Rendszerbiztonsági terv

A Hivatal vezetése az elektronikus információs rendszereihez rendszerbiztonsági tervet készít:

a) Összhangban áll a szervezeti felépítéssel.,
b) Meghatározza az EIR-t alkotó rendszerelemeket;
c) Meghatározza az EIR hatókörét, alapfeladatait és biztosítandó szolgáltatásait az ügymeneti és üzleti folyamatok szempontjából;
d) Azonosítja azokat a személyeket, akik az EIR szerepeit és felelősségeit betöltik.;
e) Meghatározza az EIR által feldolgozott, tárolt és továbbított információtípusokat.
f) Megfelelően alátámasztott módon meghatározza az EIR jogszabály szerinti biztonsági osztályát
g) Felsorolja az EIR-t érintő konkrét fenyegetéseket
h) Meghatározza az EIR működési környezetét és más EIR-ekkel vagy rendszerelemekkel való kapcsolatait vagy azoktól való függőségeit
i) Dokumentálja a rendszerre vonatkozó biztonsági követelményeket.
j) meghatározza a biztonsági alapkövetelményeket és szükség esetén az ezen felül alkalmazott kiegészítő védelmi intézkedéseket.
k) meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és azok bővítését, végrehajtja a jogszabály szerinti biztonsági feladatokat;
l) gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
m) tartalmazza az EIR-t érintő olyan biztonsággal kapcsolatos tevékenységeket, amelyek meghatározott személyek és csoportok között koordinációt vagy tervezést igényelnek.
n) a terveket a jóváhagyó felelős áttekinti és jóváhagyja a terv végrehajtása előtt.
o) Gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyek és szerepkörök megismerjék (ideértve annak változásait is).
p) Meghatározott gyakorisággal felülvizsgálja a rendszerbiztonsági tervet.
q) Frissíti a rendszerbiztonsági tervet az EIR-ben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.
r) gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A rendszerbiztonsági tervet a rendszergazda készíti el az IBF közreműködésével.

15.2 Viselkedési szabályok az interneten

A felhasználóknak TILOS a Hivatalnál:

a) Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
b) fájlcserélő vagy chat szolgáltatás használata, valamint a munkavégzéshez nem kapcsolódó letöltések végrehajtása;
c) a közösségi oldalak használata, és más, a Hivataltól idegen tevékenység végzése;
d) 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);

e) Egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám;
f) A Hivatal elektronikus levelezési rendszerét és a Hivatal tulajdonában lévő internet hálózatot feladatellátásain kívül másra használni;
g) A Hivatal informatikai hálózatán, eszközein a képernyőmegosztás, külföldi felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak nem kívánt levelezőlisták használata;
h) A Hivatal weboldala ellen bármiféle betörési kísérletet végrehajtani, illetve a szervezet hálózatát felhasználni más oldalak ellen elkövetett szabálysértés támogatására (kivéve a tervezett információbiztonsági ellenőrzéseket);
i) A hálózat erőforrásainak, a hálózaton elérhető adatok illetéktelen módosítása, megrongálása, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
j) A hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértében, pazarló módon igénybevevő tevékenység;
k) A Hivatal által biztosított azonosító és hitelesítő adatok használata külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor.

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

l) betiltott filmeket, publikációkat;
m) számítógépes játékot;
n) pornográfiát, pedofíliát, erőszakot hirdető cikkeket, publikációkat;
o) megbotránkoztató, a jó ízlés határait sértő anyagokat;
p) gyűlöletkeltésre alkalmas, vagy vallási és kisebbségi érzelmeket sértő anyagokat.

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

EIR-hez kapcsolódó viselkedési szabályok és elvárások

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

Az elektronikus információs rendszerek használata során minden felhasználó köteles:

- az információkat üzleti célhoz kötötten kezelni,
- betartani a bizalmasság, sértetlenség és rendelkezésre állás (B–S–R) elvét,
- a legkisebb jogosultság elvének megfelelően eljárni,
- a szervezet információbiztonsági szabályzatait megismerni és betartani.

Hozzáféréssel kapcsolatos viselkedési szabályok:

- Az EIR-hez való hozzáférés személyhez kötött, megosztása tilos.
- Felhasználói azonosítók és jelszavak más részére nem adhatók át.
- Ideiglenes vagy rendkívüli hozzáférés csak jóváhagyással használható.
- A hozzáférést érintő változásokat (pl. munkakör-váltás) azonnal jelezni kell.

Hitelesítés és eszközhasználat:

- Erős jelszavak és – ahol előírt – többtényezős hitelesítés (MFA) alkalmazása kötelező.
- Csak jóváhagyott, biztonságosan konfigurált eszközök használhatók.

- Ismeretlen vagy nem felügyelt eszközről EIR elérés nem engedélyezett.

Információkezelési szabályok:

- Az információk minősítésének megfelelő kezelés kötelező.
- Bizalmas adat kizárólag engedélyezett csatornán továbbítható.
- Adatok jogosulatlan másolása, továbbítása vagy nyilvánosságra hozatala tilos.

Tiltott magatartások:

Kifejezetten tilos:

- az EIR magáncélú vagy jogellenes használata.

E-mail biztonsági szabályok:

a) 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.
b) Szükséges a felhasználóhoz kötött egyéni, teljes névvel ellátott, a Hivatal által használt domain nevű egyedi e-mail címek létrehozása. (gipsz.jakab@domain.hu)
c) 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.
d) Tilos a Hivatal saját tulajdonú domain nevéhez tartozó levelezőrendszerén kívüli levelezőrendszer használata. Pl.(Freemail, Gmail)
e) 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.
f) A munkavállalóknak tilos más munkavállalók postafiókjához felhatalmazás nélkül hozzáférniük
g) A munkavállalóknak tilos a tévesen címzett, másnak szóló levelek felhasználása
h) Tilos a Hivatal által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a Hivatal elektronikus levelező rendszerében létrehozott) e-mail címre
i) 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.
j) Tilos a távozott munaktárs nevében elektronikus üzenetet küldeni.
k) A levelezési rendszerben a hozzáférést biztosító jelszavak létrehozására, kezelésére és változtatására vonatkozóan az általános jelszó használati szabályok érvényesek.
l) A munkatársak kötelesek a levelezési fiókjuk hozzáférését biztosító jelszót titkosan kezelni, azt mások tudomására hozni még a munkafolyamat felgyorsítása érdekében is tilos.
m) A munkatársak kötelesek azzonnal jelenteni a jelszavuk nyilvánosságra kerülésére utaló minden gyanút és körülményt.
n) Tilos a Hivatal levelezési rendszerében használt e-mail címmel magánérdekből, publikus rendszerekben regisztrálni, fórumokon megjelenni, hírlevelekre feliratkozni.
o) 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

p) 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.

q) 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.

r) 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.

A közösségi média használata és felelősségteljes kommunikáció

A közösségi média a kommunikációra, a közösségi interakcióra, tartalommegosztásra és együttműködésre összpontosító webhelyek, honlapok és alkalmazások gyűjtőfogalma.

A felhasználóknak mindig szem előtt kell tartaniuk, hogy a Hivatalt képviselik. Személyes közösségi média tevékenységük, még akkor is, ha közvetlenül nem munkával kapcsolatosak, következményekkel járhat a Hivatalra nézve.

A közösségi média használata során, akár személyes, akár szakmai, akár hivatali célból, a Hivatal alkalmazottainak mindig be kell tartaniuk az alábbi alapelveket:

- **Pontosság**: Győződj meg arról, hogy minden megosztott információ helyes és ellenőrzött. A munkavállalók – döntésük szerint – a közösségi média profiljukban feltüntethetik a munkahelyüket, illetve foglalkozásukat. A Hivatal elvárja munkavállalóitól, hogy amennyiben ezt teszik, az információk mindig pontosak és naprakészek legyenek. Amennyiben a Hivatal feltüntetésre kerül a munkavállaló magán profiljában, a tartalmak tekintetében kiemelt körültekintéssel kell eljárnia: a munkavállaló privát véleménye, posztja, kommentje is kihathat a Hivatal megítélésére.

- **Hitelesség**: Valódi és valósághű tartalmat ossz meg.

- **Tudatosság**: Maradj tájékozott és éber azzal kapcsolatban, hogy kivel interaktálsz a közösségi médiában, mivel sokan hoznak létre hamis profilokat vagy személyesítenek meg másokat. Ellenőrizd a másik személyiazonosságát, és legyél óvatos a lehetséges csalásokkal.

- **Megfelelőség**: Tartsd be a vonatkozó jogszabályokat és előírásokat, valamint a helyi irányelveket is. A Hivatalra vonatkozó hírek, tartalmak esetében a Hivatal elvárja

munkavállalóitól, hogy a bizalmas információkat a Hivatal hivatalos vagy felsővezetői kommunikációt megelőzően ne tegyenek közzé.

- **Titoktartás**: Az érzékeny, bizalmas és/vagy védett információk védelme.
- **Adatvédelem**: Tartsd tiszteletben az adatvédelemmel kapcsolatos rendeletet, amely biztosítja a személyes adatok optimális védelmét.
- **Tisztelet**: A közösségi médiában való kommunikáció során viselkedj tiszteletteljesen másokkal szemben. Ne feledd, hogy a közösségi médiában végzett tevékenységed akkor is tükrözheti a Hivatalt, ha a személyes fiókodat használod.

  A viselkedési szabályok betartása, a megfelelő hangnem és szóhasználat nemcsak a külső közösség irányába alapvető elvárás dolgozóinkkal szemben, hanem a munkatársak, illetve partnerek egymással folytatott belső kommunikációjára is egyaránt vonatkozik (történjen ez akár szóban, akár írásban, beleértve a belső levelezőrendszerben történő, a privát, csoportos és egyéb chat vagy videó beszélgetéseket).
- **Átláthatóság**: Fedd fel a Hivatallal való kapcsolatod, amikor a közösségi médián szakmai és hivatali felhasználás céljából lépsz kapcsolatba.
- **Viselkedj felelősen:** Munkatársainknak a közösségi médiában való megjelenésük során tartózkodniuk kell minden olyan megnyilvánulástól, amely a Hivatal jó hírnevét hátrányosan befolyásolhatja. A Hivatal elvárja munkatársaitól, hogy a közösségi médiában magánemberként történő kommunikációjuk során is a Hivatal etikai normáinak megfelelő, ahhoz méltó magatartást tanúsítsanak, különösen akkor, ha tevékenységük, illetve személyük a Hivatallal bármilyen módon összefüggésbe hozható, vagy azt a látszatot keltheti, hogy a Hivatal nevében járnak el, illetve nyilvánítanak véleményt.

A közösségi médiában közzétett minden poszt, tartalom visszakereshető, terjeszthető, képernyőkép vagy más formában megmaradhat, függetlenül attól, hogy milyen adatvédelmi beállításokat használ a profil tulajdonosa.

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

A viselkedési szabályok felülvizsgálata és frissítése évente esedékes.

15.3 Biztonsági követelmények kiválasztása

A szervezet kiválasztja az EIR számára a 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.3. ponttal összhangban a biztonsági követelményeket.

15.4 Biztonsági követelmények testre szabása

A szervezet testre szabja a kiválasztott biztonsági követelményeket.

16 Személyi 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).

Felülvizsgálat évente esedékes, illetve súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, információbiztonság szervezetrendszerét, szerepköreit érintő szervezeti változások, a használat vagy a szervezeti környezet jelentős változásai, elégtelen személyi átvilágításból adódó biztonsági incidensek esetén.

A Hivatal:

a) 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;
b) 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;
c) 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;
d) gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;
e) 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.

16.1 Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal:

- minden érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot biztonsági szempontból besorol;
- rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

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

A munkatársak kiválasztási folyamatában –külső partnerrel is együttműködve – a **jegyző** tekinti át a jelölt szakmai önéletrajzát, végzettségét, ezek összhangját a munkaköri követelményekkel, majd a **szakmai vezető** és a **jegyző** interjú keretében vizsgálják a jelölt alkalmasságát, a lehetséges kockázatokat. Szükség esetén a döntés meghozatala előtt további információkat gyűjtenek be a jelölt referenciáiról.

Az alkalmazási feltételeket a ***kinevezés, munkaszerződés***, (alvállalkozói együttműködés esetén az ***alvállalkozói/megbízási szerződés***), benne a titoktartásra vonatkozó előírásokkal, a ***munkaköri leírás*** tartalmazza.

16.2 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;
- folyamatosan ellenőrzi e pont szerinti feltételek fennállását.

16.3 Munkaköri leírások

A szervezet belefoglalja a biztonsági szerepköröket és felelősségeket a szervezeti munkaköri leírásokba.

16.4 Eljárás jogviszony megszűnése napján

A jogviszony megszűnésekor az alkalmazottnak, a szerződőknek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz, valamint elektronikus információs 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):

a) Meghatározott időn belül letiltja a rendszerhez való hozzáférést.
b) Megszünteti vagy visszavonja az adott személyhez kapcsolódó összes hitelesítő eszközt és jogosultságot;
c) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;
a) visszaveszi az érintett Hivatal elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
b) megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és a Hivatali információkhoz;
c) az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
d) a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
e) a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartására megelőző intézkedéseket tesz.

Titoktartási megállapodások

Főállású munkatársaknál a ***Titoktartási nyilatkozat*** a kinevezésben, munkaszerződésében van. Az ideiglenes és szerződéses munkatársak külön ***Titoktartási nyilatkozat*** aláírása után kezdik meg az érdemi munkát, kapnak hozzáférést információkhoz, erőforrásokhoz. A Titoktartási nyilatkozat szövegét a **jegyző** állítja össze. Az aláírt kinevezést, munkaszerződést, illetve nyilatkozatokat a jegyző a személyi mappákban őrzi.

16.5 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.

16.6 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 partner, harmadik fél minden munkával kapcsolatos adatot és információt, valamint munkájához használt eszközt (laptop, mobiltelefon, stb.) átadott, valamint a jogosultságai és hozzáférései visszavonásra kerültek.

16.7 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.

16.8 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, munkatársnak.

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

16.9 Fegyelmi intézkedések

Az informatikai rendszerek biztonságának gondatlan veszélyeztetése, az információbiztonsági 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 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, a Hivatal 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.

Személyek ismételt háttérellenőrzése szükséges fegyelmi eljárás után.

17 Kockázatkezelés

17.1 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

a) felelős a kockázatkezelési rendszer(ek) kialakításáért, működtetéséért
b) felelős a kockázatkezelési kritériumok azonosításáért
c) kinevezi a kockázatfelmérésért felelősöket, tevékenységüket felügyeli
d) gondoskodik a kockázatkezelési irányelvek betartásáról
e) biztosítja a kockázatfelméréshez és –kezeléshez a szükséges erőforrásokat
f) dönt a kockázatfelmérés elfogadásáról, kockázatok elfogadásáról, az elfogadható kockázati szintről, a szükséges intézkedésekről, figyelemmel kísérési feladatokról
g) 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:

a) felelős a kockázat-felmérési módszertan(ok) kialakításáért, jóváhagyatásáért
b) kezdeményezi az éves rendszeres felmérés indítását
c) koordinálja a kockázat-felmérési tevékenységeket
d) javaslatokat tesz kockázatkezelési, javítási intézkedésekre
e) gondoskodik a kockázatkezelési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről
f) rendszeresen tájékoztatja az IBF-en keresztül a Hivatal vezetését a kockázati szint alakulásáról, bekövetkezett kockázati eseményekről
g) felelős a szükséges oktatások megtartásáért, megtartatásáért

Az IBF

a) a kockázatfelmérésért felelős segítségével azonosítja, felméri, értékeli a területére vonatkozó kockázatokat
b) javaslatot tesz a magas kockázatok kezelésére a saját területére vonatkozóan
c) intézkedik a saját hatáskörükben kezelhető kockázatok csökkentésére, kezelésére
d) felelős a területére eső kockázatok figyelemmel kíséréséért, kezeléséért
e) a kockázatok változása, újak felmerülése esetén aktualizálja a felmérést, tájékoztatja a kockázatfelmérésért felelőst

A munkatársak

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

17.2 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.

17.3 Kockázatelemzés – Ellátási lánc

A Hivatal:

- Felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.
- Meghatározott időközönként frissíti az ellátási lánc kockázatelemzését, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatására

17.4 Sérülékenységek ellenőrzése

A Hivatal:

- Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel ellenőrzi az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek.
- Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően.

17.5 Sérülékenység-teszt

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

17.6 Sérülékenységmenedzsment – Sérülékenységi információk fogadása

A szervezet létrehoz egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket.

17.7 Kockázatokra adott válasz

A Hivatal a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira.

18 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

a) 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.

b) 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.

c) 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 az 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 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.

18.1 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.

18.2 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:

a) követelmény meghatározás;
b) fejlesztés vagy beszerzés;
c) megvalósítás vagy értékelés;
d) üzemeltetés és fenntartás;
e) kivonás (archiválás, megsemmisítés).

18.3 Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai

A szervezet megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását.

18.4 Az elektronikus információs rendszerre vonatkozó dokumentáció

A Hivatal:

Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:

- az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;
- a biztonsági funkciók hatékony használatát és karbantartását; valamint
- az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.

Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:

- a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;
- a felhasználói interakció biztonságos módját;
- a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.
- Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket;
- a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.

18.5 Biztonságtervezési elvek

A Hivatal az általa meghatározott biztonságtervezési elveket alkalmazza és megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és az EIR, valamint a rendszerelemek módosítása során.

18.6 Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal:

a) szerződéses kötelezettségként követeljük meg, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;
b) szerződésben meghatározzuk az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
c) 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.

18.7 Támogatással nem rendelkező rendszerelemek

A Hivatal:

- lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve
- a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg

19 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:

19.1 Szolgáltatásmegtagadással járó támadások elleni védelem

A Hivatal védekezik a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait és alkalmazza azokat a védelmi intézkedéseket, amelyek segítségével elérheti a szolgáltatásmegtagadással járó támadások elleni védekezés célját.

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.

19.2 A határok védelme

Az elektronikus információs rendszer:

a) ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein
b) a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a Hivatal belső hálózatától;
c) csak a Hivatal biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével 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

19.3 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.

19.4 Kriptográfiai védelem

A Hivatal meghatározza a kriptográfia szervezeten belüli felhasználási területeit és megvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat.

19.5 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.

19.6 Biztonságos név/cím feloldó szolgáltatások

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

Az EIR a név- és címfeloldási kérésekre a hiteles névfeloldási adatokon kívül az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat is biztosít. Amennyiben egy elosztott, hierarchikus névtér részeként működik, jelzi a gyermektartományok biztonsági állapotát is, és ha azok támogatják a biztonságos névfeloldási szolgáltatásokat, lehetővé teszi a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését.

19.7 Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

Az EIR eredet-hitelesítést és adatsértetlenségellenőrzést kér és hajt végre a hiteles forrásból származó név- és címfeloldó válaszokon.

19.8 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

A Hivatal számára név- és címfeloldási szolgáltatást együttesen biztosító EIR-ek hibatűrő képességgel rendelkeznek, és alkalmazzák a belső és a külső szerepkörök szétválasztását.

19.9 Folyamatok elkülönítése

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

20 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:

20.1 Hibajavítás

A Hivatal:

a) azonosítja, belső eljárásrendje alapján jelenti és kijavítja, vagy kijavíttatja az elektronikus információs rendszer hibáit;
b) telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények, potenciális mellékhatások szempontjából;
c) A biztonsági szempontból releváns szoftver- és firmware-frissítéseket kiadását követő 1 hónapon belül telepíti, vagy telepítteti;
a) 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.

20.2 Kártékony kódok elleni védelem

A Hivatal:

a) Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat.
b) frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések, új verziók jelennek meg;

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

a) 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;
b) a kártékony kód észlelése esetén blokkolja vagy karanténba helyezi azt; és riassza a rendszeradminisztrátort és az érintett Hivatal által meghatározott további személy(eke)t;
c) ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.
d) Hivatal minden munkaállomásán és szerverén jogtiszta vírusvédelmi rendszert üzemeltet, mely minden, az adathálózatról fogadott illetve oda továbbított adatállományt átvizsgál.
e) 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.
f) 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.

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

A kártékony kód észlelésekor riasztandó személyek: Rendszergazda, IBF

20.3 Automatikus frissítés

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

20.4 Az elektronikus információs rendszer felügyelete

A Hivatal:

a) 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;
b) azonosítja az elektronikus információs rendszer jogosulatlan használatát meghatározott technikák és módszerek alkalmazásával;
c) aktiválja a belső felügyeleti képességeket vagy telepíti a felügyeleti eszközöket:
d) felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
e) Elemzi az észlelt eseményeket és rendellenességeket.
f) erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
g) Jogi állásfoglalást kér a rendszerfelügyeleti tevékenységekről
h) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.
i) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

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.

A fenti feladatok biztosítása a rendszergazda feladata.

20.5 Biztonsági riasztások és tájékoztatások

Az IBF:

- Folyamatosan fogadja a meghatározott külső szervezetektől a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat;
- folyamatosan figyelemmel kíséri a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettől érkező értesítéseket;
- Szükség esetén belső biztonsági riasztásokat, tanácsokat és iránymutatásokat készít.
- Biztonsági riasztásokat, tanácsokat és iránymutatásokat ad ki a meghatározott személyeknek vagy szerepkörökben dolgozóknak, a kijelölt szervezeti egységeknek és a kijelölt külső szervezeteknek
- A biztonsági iránymutatásokat az azokban foglaltak szerint alkalmazza.

20.6 A kimeneti információ kezelése és megőrzése

A Hivatal az EIR-ben lévő és az onnan kikerülő információk kezelése és megőrzése során a szervezetre vonatkozó, hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások és működési követelmények szerint jár el.

21 Ellátási lánc kockázatkezelése

21.1 Ellátási láncra vonatkozó kockázatmenedzsment szabályzat

A Hivatal:

- A meghatározott EIR-ek, rendszerelemek vagy rendszerszolgáltatások tekintetében szabályzatot dolgoz ki a kutatás-fejlesztés, tervezés, gyártás, beszerzés, szállítás, integráció, üzemeltetés és karbantartás, kivezetés valamint a selejtezés során felmerülő ellátási lánccal kapcsolatos kockázatok kezelésére.
- Meghatározott gyakorisággal felülvizsgálja és frissíti az ellátási lánc kockázatmenedzsment szabályzatát, illetve szükség szerint annak érdekében, hogy kezelje a fenyegetéseket, valamint a szervezeti és környezeti változásokat.
- Védi az ellátási lánc kockázatmenedzsment szabályzatát a jogosulatlan közzétételtől és módosítástól.

21.2 Ellátási láncra vonatkozó követelmények és folyamatok

A Hivatal:

- Folyamatot vagy folyamatokat alakít ki annak érdekében, hogy azonosítsa és kezelje a gyengeségeket vagy hiányosságokat a meghatározott EIR ellátási láncának elemeiben és folyamataiban, a szervezet által meghatározott ellátási láncért felelős személyekkel együttműködve.
- Alkalmazza a szervezet által meghatározott ellátási lánccal kapcsolatos kontrollokat annak érdekében, hogy védje az EIR-t, rendszerelemet vagy rendszer szolgáltatást az ellátási lánccal kapcsolatos kockázatokkal szemben és csökkentse az ellátási lánccal kapcsolatos eseményekből eredő károkat és következményeket.
- Dokumentálja a meghatározott és bevezetett ellátási láncot érintő folyamatokat és kontrollokat a biztonsági szabályzatokban, az ellátási lánc kockázatmenedzsment szabályzatában és egyéb, a szervezet által meghatározott dokumentumban.

21.3 Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók

A Hivatal gondoskodik arról, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.

21.4 Beszerzési stratégiák, eszközök és módszerek

A Hivatal meghatározott beszerzési stratégiákat, szerződéses eszközöket és beszerzési módszereket alkalmaz annak érdekében, hogy kivédje, azonosítsa és csökkentse az ellátási láncból eredő kockázatokat.

21.5 Értesítési megállapodások

A Hivatal megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel.

21.6 Rendszerek vagy rendszerelemek vizsgálata

A Hivatal eseti jelleggel vagy meghatározott gyakorisággal (6 havonta) és meghatározott esetekben (súlyos biztonsági incidensek, az informatikai biztonságot (is) érintő rendkívüli események, a használat vagy szervezeti környezet jelentős változásai, új EIR-ek bevezetése, új technológia bevezetése) ellenőrzi az EIR-eket vagy rendszerelemeket az esetleges hamisítás felderítése érdekében.

21.7 Rendszerelem hitelessége

A Hivatal:

- kialakítja és bevezeti a hamisítás elleni szabályokat és eljárásokat, amelyek magukban foglalják a hamisított rendszerelemek észlelését és annak megelőzését, hogy ezek bejussanak az EIR-be; valamint
- jelenti a hamisított rendszerelemeket és azok forrását a szervezet által meghatározott külső szervezeteknek, illetve a szervezet által meghatározott személyeknek vagy szerepköröknek.

21.8 Rendszerelem hitelessége – Hamisítás elleni képzés

A Hivatal a meghatározott személyeknek vagy szerepköröknek képzést biztosít a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.

21.9 Rendszerelem hitelessége – Konfigurációfelügyelet

A Hivatal fenntartja a konfiguráció felügyeletét a meghatározott szervizelésre vagy javításra váró vagy olyan rendszerelemek esetén, amelyeket szervizeltek vagy javítottak, és arra várnak, hogy újból üzembe állítsák őket.

21.10 Rendszerelem selejtezése, megsemmisítése

A Hivatal meghatározott technikákkal és módszerekkel selejtezi a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket.

22 Záró rendelkezések

Jelen szabályzat a társaság vezetőjének jóváhagyása után 2026.02.12 napján lép hatályba azzal, hogy hatályba léptetésével egyidejűleg a korábban kiadott Információbiztonsági Szabályzat hatályát veszti.

23 A szabályzat karbantartása

A Szabályzat karbantartásáért az elektronikus információs rendszer biztonságáért felelős személy a felelős. A felülvizsgálat és frissítés szükség szerint, de legalább évente esedékes.

24 Módosítások követése

Módosítások követése:	Verziószám:	Átvizsgálta:	Dátum:
Első változat (IBSZ kialakítása)	1.0	IBF	2023-02-08
7/2024. (VI. 24.) MK rendelet szerinti frissítés	2.0	IBF	2025-03-17
Felülvizsgálat	2.1	IBF	2026-02-12

1. sz. melléklet - Felhasználói Nyilatkozat

Nyilatkozat

A FEGYVERNEKI POLGÁRMESTERI HIVATAL Információbiztonsági Szabályzatának tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

Név	Beosztás	Dátum	Aláírás
