MAXENTROP KFT

RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2018. március 1.-től.

Lezárva: 2018. február 20. Fődi Anita jegyző

Tartalomjegyzék

1. Az Informatikai Biztonsági Szabályzat

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

a) meghatározza a célokat, a szabályzat tárgyi és személyi (a Hivatal jellegétől függően területi) hatályát,
b) az elektronikus információbiztonsággal kapcsolatos szerepköröket,
c) a szerepkörökhöz rendelt tevékenységeket,
d) a tevékenységekhez kapcsolódó felelősségeket,
e) az információbiztonság hivatalrendszerének belső együttműködését

Területi hatálya:

RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL

Csongrád megye 6786 Ruzsa, Alkotmány tér 2.

Továbbá a RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL kirendeltsége(i):

6785 Pusztamérges, Móra tér 2,

6784 Öttömös, Fő utca 12

1.1. A dokumentum célja

Az informatikai biztonsági szabályzat (a továbbiakban IBSZ, vagy Szabályzat) azon alapvető biztonsági normákat és működési kereteket határozza meg, melyek érvényesítésével a Hivatal elfogadható szintre csökkentheti az általa végzett adatkezelés és adatfeldolgozás kockázatait, egyúttal hozzájárulnak a vonatkozó jogszabályokban előírt követelmények teljesítéséhez. A Szabályzat rögzíti a hatálya alá eső adatok, információk informatikai rendszeren történő adatfeldolgozásával szemben támasztott alapvető biztonsági követelményeket valamint a legfontosabb szervezeti feladatokat és felelősségi köröket.
A Szabályzat további célja, hogy iránymutatással szolgáljon a Hivatal informatikai rendszereihez hozzáférési jogosultsággal rendelkező felhasználók számára az informatikai rendszerek helyes használatáról, ismertesse a helyes és biztonságos munkavégzés szabályait, a követendő eljárásokat, továbbá rögzítse a felhasználókkal szemben támasztott elvárásokat és követelményeket.

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 köztisztviselőkre, Munka Törvénykönyve hatálya alá tartozó munkavállalóra, továbbá a Hivatalban megbízási, vagy egyéb jogviszony alapján az informatikai rendszerekhez bármilyen okból hozzáférő személyre (a továbbiakban együttesen felhasználó).
A Szabályzat területi hatálya kiterjed minden olyan épületre, helyiségre, ahol a tárgyi hatály alá eső eszközök megtalálhatók, illetve a tárgyi hatálya alá tartozó tevékenységeket végeznek.

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

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

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

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 adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

3. adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;

3a. adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

4. adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

5. adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

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

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

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

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

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

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

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

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

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

14a. EGT-állam: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) meghatározott állam;

14b. elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

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

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

17. észlelés: a biztonsági esemény bekövetkezésének felismerése;

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

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

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

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

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

23. információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét,

annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

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

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

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

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

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

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

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

31 kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;

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

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

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

35. megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

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

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

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

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

40. sérülékenységvizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

40a. súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

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

42. szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

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

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

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

46. zárt célú elektronikus információs rendszer: a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja;

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

1.5.Kapcsolódó dokumentumok

Jogszabályok

a) a munka törvénykönyvéről szóló 2012. évi I. törvény

b) a büntető Törvénykönyvről szóló 2012. évi C. törvény

c) a polgári Törvénykönyvről szóló 2013. évi V. törvény

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

e) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről (továbbiakban: technológiai vhr) szóló 41/2015. (VII. 15.) BM rendelet

f) az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet

g) a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 187/2015. (VII. 13.). rendelet

h) h)az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet

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

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

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

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

m) a szerzői jogról szóló 1999. évi LXXVI. törvény

n) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény.

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

p) 466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról

Kapcsolódó szabványok, ajánlások

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

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

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

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

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

1.6.Szerepkörök

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

RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL (vezető): az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, határoz meg a cselekvési terv teljesülése érdekében.

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

A Jegyző köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

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

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

c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

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

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

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

g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

h) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

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

j) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

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

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

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

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

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

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

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

Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó követelményeket, valamint a feladatköröket a 2013. évi L. törvény 13. §-a szabályozza részletesen.

A rendszergazda (informatikai rendszerek felügyeletével, kezelésével megbízott személy vagy szervezet) 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 licencnyilvántartás elkészítését
- részvétel az informatikai biztonsági stratégia felülvizsgálatában, megvalósításában
- új elektronikus információs rendszer bevezetése esetén a felhasználók oktatása
- a Hivatal elektronikus információs rendszereivel kapcsolatos nyilvántartásainak évenkénti felülvizsgálata.

Beosztottak, alkalmazottak, köztisztviselők: végrehajtják és betartják az utasításokat, szabályokat. Magatartásukkal segítik a hatékony és biztonságos informatikabiztonság

megteremtését. Felhasználó a Hivatal minden munkavállalója, foglalkoztatási formától függetlenül, aki az informatikai rendszereket használja. A felhasználók kötelezettsége a szabályzatban szereplő, illetve a jegyző által előírt védelmi intézkedések körültekintő betartása, alapvető elvárás a felhasználókkal szemben, hogy a napi munkavégzés során az informatikai rendszerek használata során jelen szabályzat szellemiségével összhangban járjanak el.

A felhasználó:

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

A Hivatali szerepköröket a Hivatal a munkaköri leírásokban, a Hivatal Szervezeti és Működési Szabályzatában – ügyrendjében 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 fogja 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 ezt a szerződésben.

1.7.Tevékenységek

A RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL a tv.-ben meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

1.8.Hivatalrendszer belső együttműködése

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

2. Hivatal besorolási Nyilatkozata

RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL nyilatkozatban rögzíti, hogy a 2018.01-2018.03 hó időszakban a Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával a NEIH által kiadott 41 2015 BM VHR SZVI 2.00.xlsm ürlap felhasználásával egy kockázatértékelés során végzett a 2013 évi L tv. 9. §–nak való megfelelés szerinti vizsgálat eredményeként a Hivatal biztonsági szintje a 2013 évi L tv. 9. §. (2) *d)*:

2-es (azaz kettes) besorolású

mert a szervezet vagy szervezeti egység olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe. A szervezet vagy szervezeti egység szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt.

A Hivatal a 2-es szint elérésére és fenntartására a következő folyamatokat vezeti be és tartja fenn:

- 1.1.1. a Hivatal az érintett személyi kör részére biztosítja a szervezeti, vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasításokat, belső rendelkezéseket, szabályozásokat, vagy más erre célra szolgáló dokumentumokat;
- 1.1.2. az informatikai biztonsági szabályzat részeként egy folyamatos kockázatelemzési eljárást használ, amely tartalmaz beépített ellenőrzési pontokat;
- 1.1.3. az informatikai biztonsági szabályzat egész szervezetre és működési területére vonatkozik;
- 1.1.4. az informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezető hagyja jóvá;
- 1.1.5. az informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;
- 1.1.6. a Hivatal az informatikai biztonsági szabályzat be nem tartását fegyelmi ill. jogi eljárás keretében szankcionálja;
- 2.1.1. az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;
- 2.1.2. mely tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;
- 2.1.3. ezek a folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;
- 2.1.4. ezen folyamatokat a Hivatal olyan szervezeti egységek, vagy személyek felügyelete alá rendeli, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel, vagy szervezeti egységekkel;
- 2.1.5. a folyamatokat és végrehajtásukat a Hivatal úgy dokumentálja, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi köre - megállapítható legyen.

3. Rendszerek besorolási nyilatkozata

RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL nyilatkozatban rögzíti, hogy a 2018.01-2018.03 hó időszakban, Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával egy kockázatértékelés során végzett 2013. évi L. törvénynek és a 41/2015. (VII. 15.) BM rendeletnek való megfelelés a [NEIH-OVI] Osztályba sorolás és védelmi intézkedések űrlapja (v4.60, MS Office) a 41/2015. (VII. 15.) BM rendelet alapján felhasználásával végzett vizsgálatának eredményeként a Hivatal rendszereinek biztonsági osztályai a következők:

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (az állami és önkormányzati szervek elektronikus információbiztonságáról) 7. §-a szerint „Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket besorolja egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.” A hivatkozott jogszabályhely alapján a RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL (a továbbiakban: Hivatal) által használt illetve üzemeltetett információs rendszereket biztonsági osztályba sorolja.

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

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

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

Logikai biztonsági intézkedés: az informatikai rendszerben technikailag beállított vagy kikényszerített védelmi megoldás, ilyen lehet egy megfelelő jelszóházirend beállítása vagy a hálózati tűzfalon csak a szükséges portok, protokollok engedélyezése.
Ahhoz, hogy ezeket a célokat el lehessen érni, **bizalmasság, sértetlenség** és **rendelkezésre állás** szempontjából szükséges az egyes rendszerek osztályozása.

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

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

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

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

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

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

Jelen szabályzat csak a rendszerek 2-es szinthez rendelt kötelezettségeket, elvárásokat taglalja. A 2-es szintnél magasabb a Hatóságok által meghatározott védelmi szintnek való megfelelést a Hivatal hatályos Informatikabiztonsági szabályzatának 2. sz. melléklete (RUZSAI KÖZÖS ÖNKORMÁNYZATI HIVATAL Informatika Biztonsági Szabályzat kiegészítése az ASP rendszerek informatikai biztonsági követelményekről) írja le.

A rendszerek besorolását tartalmazó részletes lista az Informatika Biztonsági Szabályzat 1. sz. mellékletében érhető el.

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

4. Adminisztratív Védelmi Intézkedések

4.1. Szervezeti szintű alapfeladatok

4.2. Informatikai biztonsági szabályzat

A jegyző megfogalmazta, dokumentálta, valamint kihirdette az informatikai biztonsági szabályzatát. Az informatikai biztonsági szabályzatot a jegyző vezetője hagyja jóvá.

Az informatikai biztonsági szabályzatát szükség szerint, de legalább három évente egyszer az informatika biztonsági rendszer felülvizsgálata során a jegyző az IB felelőssel együtt, felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági szabályzatot újra vizsgálja, szükség szerinti módosítja. A jegyző az IBSz-ben rögzíti az érintett hivatal elvárt biztonsági szintjét, valamint az érintett hivatal egyes elektronikus információs rendszereinek elvárt ás megállapított biztonsági osztályát.

4.3. Az elektronikus információs rendszerek biztonságáért felelős személy

A jegyző az elektronikus információs rendszer biztonságáért felelős személyt nevez ki (szükség esetén, akár külsős alvállalkozó), aki: ellátja az állami és hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat. A jegyző gondoskodik (alvállalkozó esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően. Továbbá szintén elvárja az erkölcsi fedhetetlenséget.

4.4. Intézkedési terv és mérföldkövei

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

4.5. Az elektronikus információs rendszerek nyilvántartása

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

a) a rendszerek alapfeladatait;
b) a rendszerek által biztosítandó szolgáltatásokat;
c) az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett Hivatal kezelésében vannak);
d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

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

A jegyző az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Elektronikus Információs Rendszerelem Leltár)* kezeli.

4.6. Kockázatelemzés

Kockázatelemzési eljárásrend

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

A Jegyző

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

Az informatikavédelmi kockázatfelmérésért a jogszabályban meghatározott képzettséggel, tapasztalattal rendelkező IBF (Informatikabiztonsági Felelős) a felelős.

Felelősségi köre:

a) felelős a kockázat-felmérési módszertan(ok) kialakításáért, jóváhagyatásáért
b) szükség szerint, kezdeményezi a 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 a Hivatal vezetését a kockázati szint alakulásáról, bekövetkezett kockázati eseményekről
g) felelős a szükséges oktatások megtartásáért, megtartatásáért

Az IBF

a) 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 Hivatal vezetését

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

Kockázatok elemzése

A jegyző 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 jegyző a jogszabályi követelményekhez igazodva a CRAMM alapú kvalitatív kockázatelemzési módszertant használja. A 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 kockázatelemzés legalább háromévenként vagy szükség esetén, soron kívül dokumentált módon történő felülvizsgálatáról.

Kockázatok kezelése

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

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

A jegyző döntései alapján az elektronikus információs rendszerek 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 IBF az új Biztonsági osztályba, biztonsági szintbe sorolás fejezetben leírtak szerint elvégezze a besorolást.

4.7 Biztonsági osztályba, biztonsági szintbe sorolás, Hivatal biztonsági szintje

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

Az elektronikus információs rendszerek biztonsági osztályba sorolását a vonatkozó jogszabályok szerint kockázatelemzés alapján végezzük el, oly módon, hogy a biztonsági osztályba sorolásnál

nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást vesszük figyelembe.

A fentiekben leírtaknak megfelelően a Hivatal az elektronikus információs rendszerek biztonsági osztályba sorolását a 4.6 pontban leírtak szerinti kockázatelemzési, kockázatkezelési feladatok eredményei alapján a NEIH által hivatalosan közzétett segédletek felhasználásával végzi el.

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

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

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

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

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

Végrehajtás gyakorisága

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

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

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

4.8 Rendszer és szolgáltatás beszerzés

Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal nem szerez be saját hatókörében informatikai szolgáltatást vagy eszközöket, és nem végez vagy végeztet olyan rendszerfejlesztési tevékenységet, amely az IB Tv. végrehajtási rendeletében meghatározott védelmi követelmények teljesítési kötelezettségét vonná maga után.

E szerint a jellemzően kis értékű, kereskedelmi forgalomban kapható, általában irodai alkalmazások, szoftverek beszerzése, illetve azok kiszolgálását segítő a hardver beszerzések történnek.

Amennyiben mégis a fent említett kategóriába eső beszerzés, fejlesztés történik, akkor a jegyző:

a) szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;
b) a vonatkozó rendelet szempontjai szerint a szerződésben meghatározza az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban, így:
    - a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is
    - a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek
    - dokumentálja a személybiztonsági követelményeke
    - ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek
    - ha az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat
c) külső és belső ellenőrzési eszközökkel ellenőrizzük, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

4.9 Üzletmenet- (ügymenet-) folytonosság tervezése

Üzletmenet-folytonosságra vonatkozó eljárásrend

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

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

Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A Jegyző által az elektronikus információs rendszerekhez készíttetett rendszerbiztonsági tervek tartalmazzák az adott saját működtetésű elektronikus rendszer (szolgáltatás) üzletmenet-folytonossági tervét is, amely:

a) összhangban áll az Informatikai Biztonságpolitikával és a Biztonságtervezési Eljárásrenddel, valamint igazodik a szervezet felépítéséhez és architektúrájához;
b) összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
c) meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;
d) 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;
e) tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, személyeket és Hivatali egységeket;
f) gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;
g) meghatározza az alapfeladatokat (a biztosítandó szolgáltatásokat és azok elvárt szolgáltatási szintjét [angolul SLA]) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
h) rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
i) jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
j) fenntartja a Hivatal által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
k) kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

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 vesszi 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).

Biztonsági eseménykezelési terv

A biztonsági események kezelésének előfeltétele azok felismerése, amelynek érdekében a Hivatal minden munkavállalója, illetve az általa használt rendszerekhez hozzáféréssel rendelkező, és minden a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személy köteles a tapasztalt rendellenességeket jelezni.

Amennyiben a bekövetkezett esemény hatására a Hivatal által használt rendszerek, illetve a bennük kezelt adatok, továbbá a tárolt információinak bizalmassága, sértetlensége vagy rendelkezésre állása sérül vagy sérülhetett, akkor azt minden esetben biztonsági eseményként kell kezelni.

A Jegyző – szükség szerint az IT üzemeltetővel, és az információbiztonsági felelőssel konzultálva – a bekövetkezett kieséses, állapot körülményeiről és hatásairól, becsült időtartamáról (helyreállítási idő) rendelkezésre álló információk mérlegelését követően dönt az esemény kezelési módjáról, amely lehet:

- kisebb hatású, az informatikai erőforrások szűk körét érintő vagy várhatóan rövid idejű erőforrás kiesés esetén (pl.: olyan hibajelenség előfordulásakor, amely helyben – esetleg távoli segítségnyújtás igénybe vételével – kezelhető, mint például egy eszköz újraindítása) a szükséges intézkedés megtételének;
- az informatikai erőforrások széles körét vagy egészét érintő (vészhelyzet) esetén a rendeletben előírt működés, nem teljesülését okozó esemény, amely a tartalék intézkedések, illetve helyreállító tevékenységek végrehajtásának elrendelését indokolja.

A biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez esetlegesen szükséges további információk (pl.: log fájlok) begyűjtésében az IT rendszert üzemeltető köteles közreműködni.

A Hivatal által használt rendszerek biztonsági eseményét az információbiztonsági felelős a vészhelyzet bekövetkezése esetén, köteles a jogszabályban meghatározott eseménykezelő felé bejelenteni.

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

A biztonsági esemény kezelésének lezárását követően szükség esetén új megelőző védelmi intézkedések bevezetésével kell a hasonló incidensek jövőbeni előfordulásának kockázatát csökkenteni.

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

4.10 Az elektronikus információs rendszer mentései

Általános követelmények

A Jegyző feladata biztosíttatni 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 jegyző 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 Hivatalban hálózati meghajtóra szabad dolgozni (ennek hiányában, a saját gép osztott könyvtárát kell használni) amelyről naponta mentés készül. A kijelölt adatok mentései automatizált módon, fizikailag elkülönített gépre történnek. Napi rendszerességgel cobian backup segítségével. Ezt csak indokolt esetben lehet mellőzni (pl. hálózat nem elérhető, program mappa helyi gépen van) a rendszer üzemeltetőjének tájékoztatásával. Ebben az esetben is gondoskodni kell az adatok mentéséről.

A fentieknek megfelelően a jegyzőnek 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 jegyző által meghatározott követelményeknek megfelelő mentési megoldás kialakítása és a mentések elkészítésével és ellenőrzésével kapcsolatos feladatok szükséges gyakorisággal történő végrehajtása az adott eszköz üzemeltetési feladataival megbízott feladata.

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.

Az elektronikus információs rendszer archíválása

Az önkormányzat tevékenységéből adódóan, ha saját rendszerein személyes, hivatali védendő adatokat kezel és dolgoz fel és ebből következően archiválási folyamatot tart fent az

elektronikus dokumentumok hosszú távú, biztonságos megőrzése, archiválása céljából, akkor a Hivatal az archíválási tevékenységét a rendeletnek megfelleő Archíválási szabályzata szerint hajtja végre.

Egyéb esetben a Hivatal maga határozza meg az archíválandó adatok körét és módját.

Az elektronikus információs rendszer helyreállítása és újraindítása

A jegyző által megbízott személy, 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.

A Hivatal az elektronikus információbiztonsággal kapcsolatos helyreállítási szabályokat, valamint az elektronikus információs rendszer helyreállításának, újraindításának menetét az érintett dokumentumban *(BCP terv)* kezeli. A mentett állományok ad-hoc visszaírása is helyreállítási tesztnek minősül.

4.11 Emberi tényezőket figyelembe vevő – személy – biztonság

Eljárás jogviszony megszűnése napján

A jegyző vagy erre jogosult megbízottja .

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

A hozzáférési jogok visszavonása

A felhasználó informatikai rendszerekhez való hozzáférési jogát visszavonja 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.

Amennyiben a felhasználó jogainak visszavonása fegyelmi vétséggel kapcsolatos és fennál a gyanúja a bizonyítékok megsemmisítésének illetve szándékos károkozásank akkor, a jogosultásg visszavonását még a fegyelmi eljárás megkezdéséről való tájékoztaás a felhasználóval előtt meg kell tenni.

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

- a Hivatal informatikai rendszerét üzemeltető megbízott értesüljön a jogosultságok megváltoztatásának szükségességéről

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

A vagyontárgyak visszaszolgáltatása

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

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

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

A munkakör változásának biztonsági kérdései

Áthelyezés esetén a jegyző a jogosultságot kiadóval együttműködve gondoskodik a munkavállaló meglévő jogosultságainak visszavonásáról, majd az új munkakörnek megfelelő új jogosultságok igényléséről, biztosításáról.

Fegyelmi intézkedések

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

A fegyelmi eljárást a vonatkozó jogszabályi rendelkezéseknek megfelelően folytatjuk le.

A szakértői jelentésről jegyzőkönyv készül, mely a fegyelmi eljárás jegyzőkönyvének része.

A jelentésnek tartalmaznia kell:

- 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 ő feladata az egyéb jogi lépések lehetőségének vizsgálata, szükség esetén azok alkalmazása.

Ha az IBSZ megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor a szabálysértőt írásban figyelmeztetheti a jegyző. A figyelmeztetés utáni ismételt szabályszegést szándékosnak tekintendő. Különösen súlyos esetben, illetve szándékosság esetén a rendszergazdák a használati jogot megvonhatják és az IBSZ megsértője a teljes információs rendszerből kitiltható. Ha szükséges, a jegyző (vagy erre feljogosított személy) fegyelmi eljárást, polgári jogi pert is indít. Amennyiben az elkövetett cselekmény a Büntető Törvénykönyv szerint bűncselekménynek

minősül, a jegyző köteles a szabályszegővel szemben feljelentést tenni, és a rendelkezésre álló bizonyítékokat az eljáró hatóságok részére átadni.

Viselkedési szabályok az interneten

a) tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
b) tiltosak az *Engedélyezési és jogosultsági szabályzatban* meghatározott, interneten megvalósuló tevékenységek (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, „sötét web" stb.) végezni;
c) a hivatali gépeken korlátozza, csak az arra munkájuk miatt jogosultaknak engedélyei a közösségi oldalak használatát, tiltja magánpostafiók elérését, és más, a Hivataltól idegen tevékenységet.

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

d) betiltott filmeket, publikációkat;
e) számítógépes játékot;
f) pornográfiát, pedofíliát, erőszakot hirdető cikkeket, publikációkat;
g) megbotránkoztató, a jó ízlés határait sértő anyagokat;
h) gyűlöletkeltésre alkalmas, vagy vallási és kisebbségi érzelmeket sértő anyagokat.

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

A jegyző a 2011.évi CXII tv. (info tv) alapján szabályozza, illetve korlátozza az internet- és email használatot. Az internet és az IT rendszer kizárólag a Hivatalai munkát segíti, tehát kizárólag munkahelyi célra engedi használni azokat. A rendszergazda (ill. erre feljogosított, megbízott személy) jogosult ellenőrizni az internet használatát, hogy betartották-e a tiltásra vonatkozó szabályokat, valamint a hálózati kommunikációt, hivatali levelezést az egyes IT eszközök jogos és szakszerű használatát. Ezt követően, a munkáltatónak joga van bármikor ellenőrizni a dolgozókat. Ilyenkor a magáncélból megnyitott honlapokba is betekinthet. Ugyanis, amennyiben a tájékoztatás ellenére a munkavállaló magáncélu oldalakat is megnyit, akkor a honlap letöltésével már hozzájárulását is adja az adatok kezeléséhez.

Az e-mailek ellenőrzése

Ha tájékoztatás keretében a munkáltató részletesen meghatározza azokat a címeket, ahonnan e-mail fogadható vagy küldhető és a levelező rendszer magáncélu használatát megtiltja, ezt követően a dolgozó teljes levelezése ellenőrizhetővé válik. A Hivatal az ellenőrzés során betartja a jogviszonyban nem álló harmadik személyek személyes adatainak védelmére vonatkozó jogait.

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

4.12 Tudatosság és képzés

Képzési eljárásrend

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

A Jegyző:

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

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 háromévente megismételjük, illetve minden olyan elektronikus információs rendszerben vagy munkakörben történő változás esetén, mely ezt indokolttá teszi.

A képzésnek kötelezően:

- felhívja a munkatársak figyelmét az informatikai biztonsági szabályzati rendszerben bekövetkezett változásokra
- ismerteti azokat a sebezhetőségeket, melyek a felhasználó nem-biztonságtudatos magatartását használják ki;
- ismerteti az azonosított, súlyosnak minősített szabálysértéseket;
- felhívja a figyelmet, hogy a megadott súlyos szabálysértések ismételt elkövetése milyen szankciókat von maga után.
- A szabályzatokban, jogszabályokban, szerződésekben előírt követelmények felfrissítése érdekében ismertetji 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 szükség szerint a jelenléti ív aláírásával igazolnak.

Alkalmazás előtt

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

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

Belső oktatások, továbbképzés

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

Képzési eljárásrend

A jegyző a vonatkozó rendelet előírásainak megfelelően, a közszolgálati jogviszonyban foglalkoztatott munkatársak részére évente tervezett a szakterületüknek megfelelő informatikabiztonsági képzéseken vesznek részt. A képzési tervek összeállítása a jegyző felelősségi körébe tartozik.

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.

5 Fizikai Védelmi Intézkedések

5.1 Fizikai és környezeti védelem

Fizikai védelmi eljárásrend

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

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

Fizikai belépési engedélyek

A Hivatal információs rendszereinek helyt adó helyiségeibe való belépésre jogosult hivatali munkavállalók (jelenléti ív) és a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek listájának elkészítéséről és kezeléséről, valamint naprakész állapotban tartásáról a Jegyző gondoskodik. A Jegyző által jóváhagyott lista írásos belépési engedélynek minősül

A jegyző:

a) összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
b) rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
c) eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
d) intézkedik a b) pont szerinti dokumentumok visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

A fizikai belépés ellenőrzése

A jegyző:

a) kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
b) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
c) gondoskodik a létesítmény információs ezsközeinek helyt adó létesítményeibe, eseti jelleggel belépők kíséretéről és figyelemmel követi a tevékenységüket;
d) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;
e) 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;
f) 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).

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.

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 épületeinek minden oldalról zárható határfelülettel kell rendelkeznie. Minden munkatárs köteles ellenőrizni a felügyelete alatt álló hivatali helyiség nyílászáróinak megfelelő működését, zárhatóságát. Rendellenesen működő, nem zárható nyílászáró javításáról haladéktalanul intézkedni kell, emiatt azt soron kívül jelezni köteles a hibát észlelő vagy arról értesülő munkatárs a Jegyző felé.

A Hivatal épületeinek ügyfelek, illetve látogatók számára biztosított bejáratain, valamint az ügyfelek és látogatók számára nyitott területein és az ügyintézésre használt, az ügyintéző munkatárs által felügyelt helyiségein kívül minden más be- és kilépésre alkalmas nyílászárót használaton kívül nyitvatartási időben is zárt állapotban kell tartani.

A belépésre jogosultak által elérhető helyiségek folyamatos ellenőrzésének biztosítása érdekében a Hivatal ügyintézésre használt helyiségeiben ügyfelek, továbbá a Hivatal egyéb, ügyfelek elől elzárt területeire, köztük a Hivatal által használt információs rendszerek elemeinek helyt adó helyiségeiben a látogatók és munkavégzés céljából a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó, stb.) kizárólag felügyelet mellett tartózkodhatnak. A felügyelet biztosítása ügyfél esetében az ügyében eljáró ügyintéző, látogató és szerződéses partner esetében a Jegyző által ezzel megbízott munkavállaló feladata.

Amennyiben a Hivatal adott telephelyén, épületében a beléptetés nem lehetséges a látogatók számára, akkor annak nyilvántartását egy feljegyzésben (napló) kell rögzíteni. A belépési napló vezetésére vonatkozó kötelezettség betartását a Jegyző jogosult ellenőrizni.

A Hivatal épületén kívül

Az alábbi szabályok érvényesek minden olyan helyiségre, ami nem 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.
- 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 az érzékeny adatokat titkosítva tároljuk (ennek egy tipikus módja, ha a laptopokon ki alakításra kerül egy titkosított partíció az érzékeny adatok tárolására)
- Nem szabad nyilvános helyen őrizetlenül hagyni.

Üres íróasztal, tiszta képernyő politika

Az irodahelyiségekben tárolt és kezelt adatok jogosulatlan felhasználása ellen minden belépésre jogosultnak fel kell lépnie. Így,

- kötelesek az általuk kezelt adathordozókat csak a használat ideje alatt maguknál tartani;
- kötelesek a papír alapú adathordozók kezelése során az iratkezelési szabályzat előírásait betartani;
- a részükre kiadott biztonsági eszközöket a hatályos szabályozások szellemében, más személyek részére nem adhatják át;
- 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;
- kötelesek minden esetben a harmadik felek felügyeletéről gondoskodni, annak érdekben, hogy az ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz;
- kötelesek 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.
- a Hivatal épületén belül, Hivatali informatikai eszközt harmadik személynek csak indokolt esetben lehet átadni (pl. laptop, előadás céljára), de ebben az esetben is gondoskodni kell róla, hogy illetéktelen ne jutthasson érzékeny adatokhoz.
- Az ügyfelek, illetve látogatók által látható területen az ügyintézés időtartama alatt a papír alapú adathordozók kezelése során kizárólag az aktuális ügyhöz szükséges iratok lehetnek elő
- kizárólag az aktuális ügyintézéshez szükséges alkalmazások, programablakok lehetnek megnyitva, (amennyiben az ügyfél rálát a képernyőre) a képernyőn.

Látogató kísérete

Az irodahelyiségekben harmadik személy nem tartózkodhat felügyelet nélkül, az üres irodákat be kell zárni, annak érdekben, hogy ellenőrizetlenül senki 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.

6 Logikai Védelmi Intézkedések

Általános védelmi intézkedések

A munkakör betöltésére való alkalmasság jogszabályban meghatározott vizsgálata, illetve az ezzel kapcsolatos feladatok elvégzése, az adott hivatali munkakör betöltéséhez szükséges iskolai végzettség, szakképzettség, szakképesítés, illetve gyakorlati idő meglétének a vizsgálata a jegyző feladata és felelőssége.

Személyi biztonság

A jegyző:

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.

6.1 Tervezés

Rendszerbiztonsági terv

A Jegyző a saját működtetésű elektronikus információs rendszereihez rendszerbiztonsági tervet készített, amely:

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

Cselekvési terv

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

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

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

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

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

Személyi biztonság

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

az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;

meghatározott gyakorisággal felülvizsgálja, és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását;

gondoskodik arról, hogy a változás esetén az eljárás szerinti frissítés, aktualizálás megtörténjen;

meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket

6.2 RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

Általános szabályok

a) A jegyző az informatikai eszközök és szoftverek beszerzésénél mindig a beszerzésekre vonatkozó Hivatali és a tv-i szabályok szerint jár el. A beszerzett számítástechnikai eszközöket és szoftvereket nyilvántartásba veszi.

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.

Hardver beszerzés

A rendszergazda a beszerzés és üzembe helyezés előtt a Hivatal Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát elvégzi. Ezen felül törekszik az egységes (homogén) eszközpark kialakítására.

Szoftver beszerzés

A rendszergazda a beszerzés és üzembe helyezés előtt a Hivatal Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát elvégzi. Ingyenes (freeware) alkalmazások esetén ellenőrzi hogy üzleti jellegű felhasználásra is szabadon használható-e. A szoftverkörnyezet kialakításánál is törekszik az egységességre (homogenitásra).

Kellékanyag beszerzés

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

6.3 A rendszer fejlesztési életciklusa

A jegyző a rendszergazda segítségével az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket.

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

A jegyző a saját működtetésű elektronikus információs rendszerhez 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).

6.4 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.

Elektronikus információs rendszerek nyilvántartása

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

- nevét;
- funkcióját;
- nyújtott szolgáltatását;

- licencszámát;
- szakterületi felelőst és elérhetőségét;
- üzemeltetési felelőst és elérhetőségét;
- továbbá releváns esetben a külső elérhetőségeket.

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

Elektronikus információs rendszerelem leltár

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

A nyilvántartásunk kiterjed:

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

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

Alapkonfigurációs nyilvántartás

A Hivatal által használt desktopok, laptopok és szerverek esetében egy alapkonfigurációs nyilvántartást készítünk, és folyamatosan aktualizálunk. A nyilvántartás elkészítéséért és frissítéséért a rendszergazda felel.

A nyilvántartásnak legalább az alábbi tételeket kell tartalmaznia:

- 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 szoftverhasználat korlátozásai

A jegyző:

a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt engedélyez, 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 állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.
d) ellenőrzi, hogy 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) engedélyével a Hivatal informatikai eszközeire szoftvereket a felhasználó is telepíthet, de tudatában kell lennie annak a informatikai biztonsági kockázataival.
f) által átruházott 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) által megbízott rendszergazda feladata rendszeres időközönként (legalább kétévente) 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 Hivatal az elektronikus információbiztonsággal, rendszer- és szoftverhasználattal kapcsolatos szabályait egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli.

A felhasználó által telepített szoftverek

A jegyző a dolgozóinak, felhasználóinak sem hardveresen, sem szoftveresen nem korlátozza a telepítési és módosítási jogosultságokat. A jegyző a Hivatal által használt EIR-ek felhasználói számára az informatikai eszközöket és erőforrásokat a hivatali munkavégzés céljára biztosítja. Így a rendszereire, valamint azok számítógépeire és egyéb komponenseire nem csak a rendszergazdák, vagy megbízottak telepíthetnek szoftvereket, de annak informatikai, információbiztonsági kockázataival tisztában kell lenniük.

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

6.5 Karbantartás

Rendszer karbantartási eljárásrend

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

Rendszeres karbantartás

A jegyző által megbízott személyek vagy vállalkozók:

a) a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
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;

Tervezett karbantartások

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

Számítógépek és szerverek: évenkénti karbantartás

Számítástechnikai hálózat: évenkénti karbantartás és tesztelés

Nyomtatók és egy eszközök: igény szerinti, de legalább évente

Adathordozók védelmére vonatkozó eljárásrend

Az adathordózónak minősülő eszközök (pl. floppy, CD, USB eszközök, külső merevlemezek, 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;

Vagyontárgyakért viselt felelősség

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

Adathordozók védelme

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

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.

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

A felhasználók saját tulajdonú adathordozóit az informatikai hálózatra csak vírusszűrés után csatlakoztathatják.

Adathordozók törlése

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

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

Informatikai nyilvántartások

Az Ibtv. előírásainak megfelelően a jegyző által megbízott rendszergazda naprakész nyilvántartást vezet a Hivatal elektronikus információs rendszereiről.

Adathordozók használata

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

6.6 Azonosítás és hitelesítés

Azonosítási és hitelesítési eljárásrend

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

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

Azonosító kezelés

A jegyző:

az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a Hivatal által meghatározott személyek vagy szerepkörök jogosultságához köti. Az így kisztott jogokat a felhasználók kötelesek használni attól nem térjhetnek el.

A hitelesítésre szolgáló eszközök kezelése

A Jegyző 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 a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
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 elektronikus információs rendszer telepítése során;
f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
i) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

A hitelesítésre szolgáló eszköz visszacsatolása

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

Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett hivatalon kívüli felhasználókat és tevékenységüket. A jegyző az Engedélyezési és jogosultsági szabályzatba leírtak szerint biztosíthat távoli hozzáférést a rendszereihez, melyről külön nyilvántartást kell vezetni. A szervezet jelenleg egyik rendszeréhez sem biztosít hozzáférést külső felhasználók számára, csak a hálózatának elemeihez.

6.7 Hozzáférés ellenőrzése

Hozzáférés ellenőrzési eljárásrend

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

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

Felhasználói fiókok kezelése

A jegyző:

a) meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;

…értesíti a fiókkezelőket, ha:

a) a felhasználói fiókokra már nincsen szükség;
b) a felhasználók kiléptek vagy áthelyezésre kerültek;
c) az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

…feljogosít az elektronikus információs rendszerhez való hozzáférésre:

a) az érvényes hozzáférési engedély,
b) a tervezett rendszerhasználat,

c) az alapfeladatok és funkcióik alapján;

A jegyző évente vagy a fiók és vagy felhasználó változása esetén felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot.

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.

Hozzáférés ellenőrzés érvényesítése

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

Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

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

Külső elektronikus információs rendszerek használata

A jegyző 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) A Hivatal, semmilyen külföldi felhő-alapu tárhelyszolgáltatást a nemzeti adatvagyon védelme érdekében nem vehet igénybe, azt technikailag nem teszi lehetővé (pl. dropbox, gmail, drive) Ettől eltérően csak a NEIH rendelkezhet, annak írásos engedélyéhez köti.

Nyilvánosan elérhető tartalom

A jegyző:

a) kijelöli a Hivatal vezető beosztású munkatársát, aki jogosult a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivataltól kapcsolatos bármely információ közzétételére. A Hivatalban csak a Jegyző által engedélyezett információkat lehet közzétenni. Minden más információ közzététele TILOS!
b) a kijelölt személyt képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;
c) közzététel előtt átvizsgálja a javasolt tartalmat;
d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.
e) A jegyző 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 (domaine.hu) tartalommenedzsmentjét a egy külsős megbízott, megbízási szerződés keretében végzi.
h) A hivatali ügyintézéssel kapcsolatos dokumentációk, határozatok, rendeletek a jegyző, illetve a polgármester jóváhagyását követően kerülnek nyilvánosságra.

i) A publikált információk csak nyilvános adatokat és információkat tartalmazhatnak. A jegyző legalább évente áttekinti a honlapot és nem nyilvános adat kikerülése esetén eltávolítatja azt.
Az informatikabiztonsági felelős időszakos ellenőrzés keretében szintén ellenőrzi a honlap jogszabályoknak való megfelelését.
Amennyiben a Hivatali honlap, külsős adatokat felhívásokat, egyéb információkat tartalmaz, annak valódiságtartalmáért a külsős által megadott (vagy felhelyezett) adatok tartalmáért a külsős tárhelybérlő a felelős. A jogszabályba vagy közerkölcsbe ütköző adatok információk kihelyezését megtagadjuk.

6.8 Rendszer- és információsértetlenség

Rendszer- és információsértetlenségére vonatkozó eljárásrend

A rendszer- és információsértetlenség megvalósítása során a jegyző az IBSZ követelményei szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

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

Hibajavítás

A jegyző vagy általa megbízott személy:

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 szempontjából;
c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepíti, vagy telepítteti;
d) beépíti a hibajavítást a konfigurációkezelési folyamatba.

Kártékony kódok elleni védelem

A jegyző vagy általa megbízott személy:

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

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

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 riasztja 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.
g) A felhasználónak tilos a biztonsági szoftvereket kikapcsolni, működésüket módosítani,

Az elektronikus információs rendszer felügyelete

A jegyző a rendelkezésre álló információbiztonsági eszköz és alkalmazás segítségével:

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;
c) felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
d) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
e) erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
f) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

A kimeneti információ kezelése és megőrzése

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

6.9 Naplózás és elszámoltathatóság

Naplózási eljárásrend

A jegyző az általa üzemeltetett EIR-ekre vonatkozó az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként, külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben határozza meg, az alábbi általános követelmények figyelembevételével:

Naplózható események

A jegyző az érintett elektronikus információs rendszerre vonatkozó rendszerbiztonsági tervben:

a) meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét.
b) egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő Hivatali egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
c) megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

d) A számon kérhetőség és hibakezelés biztosítása érdekében az informatikai eszközöknek az informatikai rendszer működéséről és különösen az informatikai biztonsági eseményekről helyi naplóállományt generál.
e) 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.
f) 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, az jegyző tájékoztatása mellett. A naplóállományokat meghibásodás vagy biztonsági incidens esetén, eseti jelleggel vizsgálja. Meghibásodás esetén a naplóállományok vizsgálata a hibajavításban eljáró üzemeltető feladata. A naplóállományok rendszeres átvizsgálása, a rendszerek naplóállományainak mentése, archiválása alapesetben nem elvárás

Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekből gyűjt elegendő információt ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele. A Hivatal a naplózással kapcsolatos részletes szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági szabályzat)* kezeli

Időbélyegek

A jegyző a Hivatal által üzemeltetett rendszereknél és hálózatnál, elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a Hivatal által meghatározott időmérési pontosságnak. Jelenleg ez a funkciót nem értelmezhető a Hivatalban.

A napló információk védelme

A jegyző a Hivatal által üzemeltetett rendszereknél az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

A naplóbejegyzések megőrzése

A jegyző a Hivatal által üzemeltetett rendszereknél a naplóbejegyzéseket meghatározott – a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő – időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

Naplógenerálás

A jegyző a Hivatal által üzemeltetett rendszereknél:

a) biztosítja a naplóbejegyzés generálási lehetőségét a 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 szükséges eseményekre, a meghatározott tartalommal.

A dolgozókat a belépéskor, és az éves oktatás keretében tájékoztatjuk, hogy mit, mikor, hogyan miért, naplózunk. Tájékoztatjuk, hogy ehhez nem kell engedély, csak tájékoztatás. Indokoljuk,

hogy a hivatali gépeket, csak hivatli tevékenységre, munkára lehet használni. Továbbá tájékoztatjuk a jogszabályban biztosított jogairól.

6.10 Rendszer- és kommunikációvédelem

Rendszer- és kommunikációvédelmi eljárásrend

A rendszer- és kommunikációvédelem megvalósítása során a jegyző az IBSZ követelményei szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

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

A határok védelme

A jegyző a belső hálózat védelmének biztosítása érdekében határvédelmi megoldást (tűzfal) alkalmaz a hálózati forgalom felügyeletére, irányítására. Az elektronikus információs rendszer:

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

Kriptográfiai kulcs előállítása és kezelése

A Hivatal nem végez olyan infokommunikációs tevékenységet, amely kriptográfiát követelne meg.

Kriptográfiai védelem

A Hivatal nem végez olyan infokommunikációs tevékenységet, amely kriptográfiát követelne meg.

Együttműködésen alapuló számítástechnikai eszközök

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

Folyamatok elkülönítése

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

Dátum: 2018. február 20.

Fődi Anita

jegyző

Szerzői jogok