Ikt.szám: I/959-8/2018.

Szilsárkányi Közös Önkormányzati Hivatal

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Jóváhagyom:

dr. Horváth Martina
jegyző

Szilsárkányi Közös Önkormányzati Hivatal * Szilsárkány *

Érvényes: 2019. január 1-től

TARTALOMJEGYZÉK

I.
INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet értelmében a szervezet informatikai biztonsági szabályzatát (továbbiakban IBSZ) az alábbiak szerint adom ki.

1. A szabályzat célja

Az informatikai biztonság az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága (confidentiality), sértetlensége (integrity) és rendelkezésre állása (availability) biztosított (CIA elv), valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Ahol:
- bizalmasság: csak az arra jogosultak ismerhetik meg az információt;
- sértetlenség: az információ tartalma és formája az elvárttal megegyezik, beleértve az is, hogy az elvárt forrásból származik (hitelesség), igazolható, hogy megtörtént (letagadhatatlanság), egyértelműen azonosítható az információval kapcsolatos műveletek végzője (elszámoltathatóság), továbbá rendeltetésének megfelelően használható;
- rendelkezésre állás: az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva;
- zártság: az összes releváns veszélyt (fenyegetést) figyelembe veszi;
- teljes körűség: a rendszer minden elemére kiterjed a védelem;
- folytonosság: időben folyamatosan megvalósul a védelem;
- kockázatokkal arányosság: a rendszer várható működésének időtartamában a védelem költsége arányban van a lehetséges kárral.

Az információbiztonság tágabb fogalom, mint az IT biztonság. Beleértjük az információ minden – nem csak elektronikus – megjelenési formájának, az információs szolgáltatásoknak és az ezeket biztosító információs rendszereknek a védelmét.

Az IBSZ a Hivatal szervezeti szintű szabályozó rendszerének alapvető eleme.
A Közös Hivatal által kezelt adatok biztonságának, továbbá az információbiztonsági követelményeknek való megfelelés biztosítása.
További cél, hogy a szabályzat egységes szerkezetbe foglalja a használatban lévő informatikai rendszerekkel és annak a felhasználóival szemben támasztott informatikai biztonsági követelményeket.

Az IBSZ-ben szereplő követelményeket a hatályos jogszabályi rendelkezések, a Hivatal szervezeti és Működési Szabályzata és Ügyrendje szerint kell használni. A tudatosság, szervezettség, hatékonyság és a technikai megoldások segítségével növelni kell az információbiztonságot. A tájékoztatás, oktatás, megelőzés, felderítés, szankcionálás eszközeivel segíteni szükséges az intézkedések érvényesítését.

2016.szeptember 3-án hatályba lépett az önkormányzati ASP rendszerről szóló 257/2016. (VIII.31.) Kormányrendelet, amely alapján a Hivatalnak 2017. január 1-től csatlakoznia kellett az ASP önkormányzati adórendszeréhez és a gazdálkodási rendszeréhez, valamit 2017. október 1-től az ASP valamennyi szakrendszeréhez.

Az önkormányzati ASP rendszer elemei:
a) szakrendszerek,
b) keretrendszer,
c) támogató rendszerek és
d) az Mötv. 114. § (4) bekezdése szerinti önkormányzati adattárház.

Az önkormányzati ASP rendszer szakrendszerei:
a) iratkezelő rendszer,
b) önkormányzati települési portál rendszer,
c) az elektronikus ügyintézési portál rendszer, ideértve az elektronikus űrlap-szolgáltatást,
d) gazdálkodási rendszer,
e) ingatlanvagyon-kataszter rendszer,
f) önkormányzati adórendszer,
g) ipar- és kereskedelmi rendszer,
h) hagyatéki leltár rendszer.

2. A szabályzat hatálya

A szabályzat hatálya kiterjed a **Szilsárkányi Közös Önkormányzati Hivatal szervezetre.**

2.1. Személyi hatály:

Az Informatikai Biztonsági Szabályzat (továbbiakban IBSZ) kiterjed a Közös Hivatal köztisztviselőire, ügyintézőire, a hivatal valamennyi munkatársára, valamint azokra a személyekre, akik részt vesznek az önkormányzatnál keletkező, tárolt, illetve továbbított adatok kezelésében.
A szabályzat hatálya kiterjed a választott tisztségviselőkre (polgármester, alpolgármester, képviselők), a Munka Törvénykönyve szerint foglalkoztatott dolgozókra, a Hivatallal szerződésben kapcsolatban álló természetes személyekre és jogi személyekre, valamint más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

2.2. Tárgyi hatály:

Az IBSZ kiterjed a Közös Hivatalnál kezelt, keletkezett információkra, az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemekre, amely felhasználja,

feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja az önkormányzatnál keletkező, illetve felhasznált adatokat. Kiterjed továbbá a rendszerelemek dokumentációira.
Az IBSZ tárgyi hatálya kiterjed az önkormányzati ASP központ által nyújtott szakrendszerek felhasználói oldali komponenseire:

- munkaállomások
- a munkaállomásokon futó szoftverekre
- kártyaolvasókra
- e-Személyire

3. Az IBSZ felülvizsgálata

Az IBSZ-t szükség szerint, de legalább évente felül kell vizsgálni.
Határidő: tárgyévet követő év január 31.
A felülvizsgálat elvégzéséért és a szabályozás jóváhagyásáért a jegyző a felelős.
Az IBSZ felülvizsgálatában az információbiztonsági felelős közreműködik.

4. Értelmező rendelkezések:

1. *Adat:* az információ hordozója, megjelenési formája, értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) jelsorozat; olyan jelsorozat, amelyből információ nyerhető ki.
2. *Adatállomány:* adathordozón tárolt, jelképes névvel ellátott adathalmaz.
3. *Adatbázis:* a megfelelő kezelőszoftverrel rendszerbe szervezett, egy vagy több adatállomány.
4. *Adatbázis-motor:* adatbázis-kezelő programok közös, szabvány szerint működő, az adatbázisok elemeit kezelő, hozzáférést, adatfeldolgozást, keresést és egyéb funkciókat kiszolgáló alapmodulja. Az adatbázis-motor az adatbázis kezelő programok vázaként működik, ezek moduljait is vezérli, működésüket alapszabályok szerint definiálja, kiegészítő funkciókat, illesztéseket szabályozza.
5. *Adathalmaz:* valamilyen feldolgozás részére rendelkezésre álló adatok összessége.
6. *Adatátvitel:* adatok szállítása összeköttetéseken, összekötő utakon, informatikai eszközök között.
7. *Adatbiztonság:* az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
8. *Adatbiztosítás:* szélesebb értelemben azon intézkedések összessége, amelyek célja az adatbiztonság szavatolása. Szűkebb értelemben az az intézkedés, amelynek megvalósítása során az adatok biztonsági okokból (rendelkezésre állás és sértetlenség) rendszeresen mentésre kerülnek.
9. *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.
10. *Adatkezelés:* az adatokon végzett tevékenység (az adatok gyűjtése, rendszerezése, feldolgozása, módosítása, archiválása, törlése, stb.).

11. *Adatvédelem:* az adatok jogosulatlan megszerzésének, illetve manipulálásának megakadályozására irányuló intézkedések összessége.
12. *Alkalmazói program (alkalmazói szoftver):* olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja.
13. Adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;
14. Auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;
15. *Bejelentkezés:* az informatikai rendszer és egy felhasználó között olyan kapcsolat kezdeményezése az utóbbi által, amelynek során számára az informatikai rendszer funkcióinak használata lehetővé válik, valamint a felhasználó egyértelműen azonosítható lesz.
16. 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;
17. *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;
18. *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;
19.*Biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;
20. *Biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
21. *Biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
22.*Biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
23. *Elektronikus levelező rendszer:* olyan informatikai rendszer, amely az elektronikus levelek (e-mail) küldésére és fogadására szolgál. Alapelemei: felhasználói postafiók, technikai fiók, terjesztési lista, nyilvános naptár, jogosultságok (betekintési, szerkesztési, meghatalmazotti levélküldési, tulajdonosi, adott email címről levélküldési jog). Saját üzemeltetésű, illetve külső szolgáltatótól átvett szolgáltatás keretében vehető igénybe.
24. *Elektronikus levelező rendszer – felhasználói postafiók:* az Intézmény által a munkatársak (felhasználó) munkavégzés céljából rendelkezésére bocsátott elektronikus postafiók, amelyhez a felhasználó hozzáféréssel rendelkezik és a munkakörében meghatározott feladatok elvégzéséhez használja kapcsolattartásra az Intézmény, illetve a Főigazgatóság és a kirendeltségek munkatársaival, valamint külső személyekkel. A felhasználói fiók meghatározottan egyetlen személyhez kötődik. A postafiók főbb elemei: Beérkezett üzenetek mappa és almappái, Elküldött üzenetek mappa és almappái, személyes naptár.
25. *Elektronikus levelező rendszer – technikai fiók:* olyan elektronikus postafiók, amely jellemzően több felhasználó által használt (a felhasználók előre definiált jogosultsági szinttel férnek hozzá). A technikai fiók egy megadott struktúrájú megnevezéssel rendelkezik.
26. *Elektronikus levelező rendszer – Nyilvános Naptár:* az elektronikus levelező rendszer speciális objektuma, amelyet a személyes naptárral megegyező feladatot lát el. A naptárhoz

egy adott felhasználó előre definiált hozzáféréssel (betekintési joggal, szerkesztési joggal, nincs jogosultsága) láthatja az objektum tartalmát (naptárbejegyzéseket).

27. *Elektronikus levelező rendszer – betekintési jogosultság:* az elektronikus levelező rendszerhez tartozó alap jogosultságszint, amelyet felhasználói postafiók mappájához, technikai postafiókhoz valamint nyilvános naptárhoz rendelhetünk. Ezzel a jogosultsággal a felhasználó a mappák tartalmába betekintést nyer, elemein változtatni nem tud, az elemek áthelyezése, törlése, új almappa létrehozása nem megengedett.

28. *Elektronikus levelező rendszer – szerkesztési jogosultság:* az elektronikus levelező rendszernek az alapszintnél magasabb jogosultsági szintje, amelyet felhasználói postafiók mappájához, technikai postafiókhoz valamint nyilvános naptárhoz rendelhetnek. Ezzel a jogosultsággal a felhasználó a mappa elemeit módosíthatja, törölheti, almappákat hozhat létre.

29. *Elektronikus levelező rendszer – meghatalmazotti levélküldési jog:* az elektronikus levelező rendszer speciális jogosultsága, amelyet felhasználói postafiókhoz, illetve technikai fiókhoz rendelhetnek. A jogosultsággal az adott felhasználó egy másik felhasználó (vagy technikai fiók) nevében elektronikus levelet küldhet. Ekkor a levél címzettjében az „XY" Meghatalmazó: „Z felhasználó" vagy „a technikai fiók neve" szerepel. Az elküldött levél a meghatalmazott felhasználó elküldött üzenetek mappájába kerül tárolásra.

30. *Elektronikus levelező rendszer – tulajdonosi jog:* az elektronikus levelező rendszerben lévő legmagasabb jogosultsági szint. Egy felhasználó a személyes felhasználói postafiókján tulajdonosi jogosultsággal rendelkezik. E jogosultság birtokában képes a postafiók elemeihez más felhasználók részére jogosultságokat biztosítani.

31. *Elektronikus levelező rendszer – adott e-mail címről levélküldési jog:* az elektronikus levelező rendszer speciális jogosultsága, amelyet felhasználói postafiókokra illetve technikai fiókokra állíthatunk. Az a felhasználó, aki ezzel a jogosultsággal rendelkezik, úgy küldhet levelet egy másik felhasználó illetve a technikai fiók nevében, hogy a levél címzettje nem látja azt, hogy ezt a levelet ténylegesen nem a levél feladója, hanem más felhasználó küldte. A jogosultság csak megfelelő indoklással és annak a felhasználónak a személyes beleegyezésével adható ki, akinek az e-mail címéről küldeni kívánnak. A jogosultság igénylése kizárólag írásban történhet.

32. *Elektronikus levelező rendszer – terjesztési lista:* az elektronikus levelező rendszer olyan objektuma, amely arra szolgál, hogy egy levél több felhasználó (címzett) részére is elküldésre kerülhessen anélkül, hogy a tényleges címzetteket egyesével kellene a levél címzettjei közé felvenni. A terjesztési lista alapesetekben felhasználókat, de igény szerint további terjesztési listákat tartalmazhat. Megkülönböztetünk központilag kezelt és helyi (a felhasználó saját célfeladatára létrehozott) terjesztési listát.

33.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;

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

35. Észlelés: a biztonsági esemény bekövetkezésének felismerése;

36.Felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;

37. 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;

38. 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;
39. Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
40. 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;
41. Helpdesk rendszer: olyan információs rendszer, amely a felhasználók hibabejelentéseinek és egyéb informatikát érintő bejelentéseinek kezelését és az intézkedések dokumentálását és nyomon követését teszi lehetővé.
42. *Hozzáférés:* olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.
43. Informatikai biztonságpolitika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;
44. Informatikai biztonsági stratégia: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;
45. 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;
46.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 működéséhezés működtetéséhez;
47. Kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;
48.Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;
49. Kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
50.Kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;
51. Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;
52. Korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;
53. 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;

54. Logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
55. 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;
56. Megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;
57. Reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
58. Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
59. 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;
60. Sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;
61. Sérülékenységvizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;
62. Számítógépes incidenskezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];
63. Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;
64. Üzemeltető: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;
65. Védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;
66. Zárt célú elektronikus információs rendszer: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;
67. Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

5. Alapvető elektronikus információbiztonsági követelmények

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:
a) számítástechnikai rendszerek és hálózatok;

b) helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;
c) rádiós vagy műholdas navigáció;
d) automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő, távmérő, távérzékelő és telemetriai rendszerek);
e) a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

Egy elektronikus információs rendszernek kell tekinteni az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön (környezeti infrastruktúra, hardver, hálózat), egymással összefüggő eljárásokkal (szabályozás, szoftver és kapcsolódó folyamatok) azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttesét.

Az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell
a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása
zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.
Az elektronikus információs rendszernek megfelelő védelme körében a szervezetnek biztosítani kell.
a) a megelőzést és a korai figyelmeztetést,
b) az észlelést,
c) a reagálást,
d) a biztonsági események kezelését.

6. Az elektronikus információs rendszer biztonsági osztályba sorolása

A technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelmények a 41/2015. (VII. 15.) BM rendeletben kerültek rögzítésre.

- az elektronikus információs rendszerek biztonsági osztályba sorolása a rendelet 1. melléklet alapján,
- az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása a rendelet 2. melléklet szerint,
- az elvégzett besorolás alapján az elektronikus információs rendszerrel rendelkező szervezet a rendelet 3. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket a rendelet 4. mellékletben meghatározott módon teljesíti.

Az elektronikus információs rendszer biztonsági osztályba sorolását az elektronikus információs rendszer biztonságáért felelős személy végzi.

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

A Szervezet számára a jogszabályban előírt biztonsági osztály: 4.

Szervezetünk a számára jogszabályban előírt 4. biztonsági osztály előírásait alkalmazza.

Szakrendszer	Biztonsági osztály
Adó rendszer	4
Keretrendszer	4
Gazdálkodási rendszer	3

7. Az elektronikus információs rendszer biztonságáért felelős személyek feladatai

Az informatikai biztonság megfelelő kialakításának egyik követelménye a biztonsággal kapcsolatos szerepkörök szétválasztása.
A Hivatal minden munkatársa, szerződésben lévő informatikai alvállalkozója és természetes személy köteles az IBSZ előírásait betartani.

A Hivatal információbiztonsági feladatainak ellátása során a következő személyek látnak el feladatokat:

- jegyző,
- információbiztonsági felelős, (IBF)
- rendszergazda,
- adatgazdák,
- szervezeti egység vezetők,
- felhasználók.

7.1. A jegyző feladatai:

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,
f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
j) 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,
k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a törvényben és az IBSZ-ben foglaltak szerződéses kötelemként teljesüljenek,
m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:
a) az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére."

7.2. Információbiztonsági felelős feladatai:

Az elektronikus információs rendszer biztonságáért felelős személy az információbiztonsági felelős (IBF), akit a feladattal a jegyző bíz meg.

Az információbiztonsági felelős a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért felelős.

Ennek körében:
a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi vagy irányítja az *a)* pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Üzemeltetéssel kapcsolatos feladatai körében:

- Biztosítja a rendszerfelügyeletet
- Üzemelteti a rá bízott elektronikus információs rendszereket
- Vezeti az IBSZ-ben előírt nyilvántartásokat

Az elektronikus információs rendszer biztonságáért felelős személy az elektronikus információs rendszert érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az alábbiak teljesülését:
a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,
b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők a törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.
Az elektronikus információs rendszer biztonságáért felelős személy jogosult a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.
A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.
A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

Az elektronikus információs rendszer biztonságáért felelős személy a feladatait megbízás alapján látja el, adatai a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) számára jelentésre kerülnek.

Az információ biztonsági felelős szervezetünknél:

Németh László külső szolgáltató Koonkoord KFT 9023 Győr, Fehérvári u. 17/B

Az elektronikus információs rendszer biztonságának megteremtésében közreműködik:

Janik Zsolt rendszergazda, külső szolgáltató Koonkoord KFT 9023 Győr, Fehérvári u. 30-385-32-50

zsjanik@konkoord.hu

7.3. Az adatgazda

Az adatgazda annak a szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály adat kezelését vagy nyilvántartás vezetését elrendeli.
A Szilsárkányi Közös Önkormányzati Hivatal egységes gazdasági szervezettel működik, adatgazda valamennyi nyilvántartás tekintetében a jegyző.

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

Az adatgazda meghatározza a hozzáférési jogosultságokat, a szükséges, minimális jogosultságok elvére figyelemmel. Biztosítja, hogy mindenki annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges.

7.4. Önkormányzati ASP adminisztrátor

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

- az adott tenant felhasználóinak felvétele és szakrendszeri szerepkörökhöz rendelése, annak adminisztrációja és karbantartása,
- kapcsolattartóként az adott tentant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, a tanúsítványokat hordozó tokenek csoportos átvétele és a felhasználók közötti kiosztása.

7.5. A felhasználók jogai, kötelességei és felelőssége

A felhasználók jogai:

A számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használata.
A munkájához szükséges adatállományok elérése.

A felhasználók kötelességei

Valamennyi felhasználó köteles értesíteni a felettesét, vagy az informatikai biztonsági felelőst a következő esetekben:

- az informatikához kapcsolódó tevékenység fennakadása, megszakadása
- olyan adatokhoz fér hozzá, amihez nem illetékes
- információbiztonsági esemény.

A felhasználók kötelesek bizalmasan kezelni a felhasználói azonosítókat, jelszót, eToken-t, kulcsot, vagy bármely egyéb a Hivatal informatikai rendszereihez és adataihoz hozzáférést biztosító eszközt. A személyi azonosító kódokat, jelszavakat szigorúan titokban kell kezelni.

A felhasználók felelőssége

- A felhasználó felel az általa az elektronikus információs rendszerben végzett műveletekért,
- a rendszer szakszerű kezeléséért,
- a személyi használatra átvett eszközök szakszerű kezeléséért,fizikai védelméért,
- a személyre szóló kártyájának védelméért.

A felhasználó számára büntetőjogi, ill. munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, más jelszavának kipróbálása, ill. ennek a kísérlete is.

8. Az ASP rendszerhez csatlakozás

A 257/2016. (VIII. 31.) Korm. rendelet 2. melléklete tartalmazza a minimumkövetelményekhez tartozó megfelelés elvárását. Ez alapján ki lehet alakítani azt az informatikai infrastruktúra környezetet, amellyel biztosított az ASP rendszerhez történő csatlakozás a következők alapján.

Az informatikai környezet fő komponensei:

- Munkaállomások beüzemelés
- Nyomtatók üzembe állítása
- Hálózati aktív eszközök beüzemelése, hálózat kiépítése
- Vírusvédelmi rendszer beüzemelése
- Tűzfal beüzemelése
- Internetkapcsolat üzembe állítása

Az infrastruktúra felállításának főbb feladatai

- Tenant létrehozása a Keretrendszerben (ASP. KERET), Tenant adminisztrátor felvétele a Keretrendszerben (ASP.KERET).
- Adatbázisok létrehozása a Gazdálkodási (ASP. GAZD) és szakrendszerben.

- Tenant felhasználók felvétele és szerepkörök összerendelése a Keretrendszerben (ASP. KERET).
- Tanúsítványok elkészítése és hozzárendelése.
- Tanúsítványok kiosztása önkormányzati felhasználók között.

IT biztonsági feltételek megteremtése

- Önkormányzati biztonsági szint meghatározása.
- A meghatározott biztonsági szinthez kapcsolódó védelmi intézkedések biztosítása.
- Információbiztonsági szabályozások kialakítása, szükség szerinti módosítása, jóváhagyása, kihirdetése.
- Biztonsági auditra való felkészülés.
- ASP-vel kapcsolatos audit tevékenység csak a Hatóság írásbeli engedélyével végezhető el. Erről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.
- ASP rendszeren külsős Fél, szervezet nem végezhet sérülékenységi vizsgálatot a Hatóság írásbeli engedélye nélkül. Ezen vizsgálati tényről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.

9. Fizikai biztonság, őrzés, védelem megteremtése ASP-ben

A fizikai védelem főbb részei a következők lehetnek:
- mechanikai védelem;
- elektronikai jelzőrendszer;
- élőerős védelem;
- beléptető rendszer;
- biztonsági kamera rendszer;
- villám és túlfeszültség védelem;
- tűzvédelem.

9.1. Szervezetünk intézkedései a fizikai biztonság megteremtése érdekében:

A Közös Hivatal épülete munkaidőn túl zárva van. Hivatali helyiségeink riasztó berendezéssel még nincsenek felszerelve, de a költségvetés függvényében tervezzük a riasztó beszerzését.

A szerver tárolására szolgáló helyiség az ügyfélforgalomtól elkülönült helyiségben található, ahová az illetéktelenek számára a belépés tilos. Tűzvédelmi szabályzattal rendelkezünk, amelynek betartását a jegyző ellenőrzi. Tűzvédelmi berendezéseinket rendszeresen felülvizsgáltatjuk. Villám és túlfeszültség védelmet a berendezéseinkre biztosítjuk. Évente tűzvédelmi és munkavédelmi oktatásban részt veszünk. Biztosítjuk a tűzvédelmi előírások betartását.
A földszinti ablakokon vasrács még nincs, da a költségvetés függvényében tervezzük annak felszerelését.

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

hatékonysága ne romoljon. A védelmi intézkedések biztosítsák, hogy a különböző környezeti hatás miatt keletkező meghibásodások csökkenjenek.

A Hivatal területére a normál háztartási vegyi anyagokon, tisztítószereken túl vegyi anyagot, robbanóanyagot behozni tilos;
A monitorokat úgy kell elhelyezni, hogy ki lehessen zárni azok illetéktelen leolvasását
Különös figyelmet kell fordítani az önkormányzati ASP rendszert elérő munkaállomások elhelyezésére, gondoskodni kell az illetéktelen hozzáférések megakadályozásáról.

Az információi biztonsági felelős rendszeresen félévente ellenőrzést hajt végre, amelynek az eredményt jegyzőkönyvben rögzíti. A jegyzőkönyvet az ASP Szolgáltatási szerződésben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre átadjuk.

Tápáramellátás

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

A kábelezés biztonsága

Biztosítani kell az elektromos és adatvezetékek megszakadás és a rongálások elleni megfelelő védelmét. A hálózati zavarok okozta hibák elkerülése érdekében az erősáramú vezetékeket el kell különíteni a kommunikációs hálózattól. A kábelstruktúra legyen érzéketlen az elektromos hálózati zavarokra.

„Üres asztal - üres képernyő" szabály

Az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden dolgozónak ismernie és alkalmaznia kell a jelen pontban leírtakat:
a) a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);
b) a felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;
c) a zárolás elfelejtésének esetére jelszóvédett, automatikus zárolást kell beállítani, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;
d) a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a munkaállomást;
e) a felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget szerint be kell zárniuk, ha a helyiségben senki nem tartózkodik;
f) ügyfelet irodában felügyelet nélkül hagyni tilos.

9.2. Felügyelet alól kikerülő eszközök

Szerviz részére eszközt csak az informatikai biztonsági felelős ill. rendszergazda adhat át. Szervizbe történő szállítás esetén a szerviz által adott szállítólevelet a rendszergazda őrzi meg. Szervizbe történő szállításkor vagy garanciális javítás esetén - jegyzőkönyv felvétele mellett – a rendszergazdának gondoskodnia kell az adatokat tartalmazó adathordozók törléséről.
A munkatársak részére hosszú távú használatra kiadott nagy értékű eszközökről (pl.: laptop) a Hivatalnak nyilvántartást kell vezetnie. Ezen eszközöket a munkatársak korlátozás nélkül ki és beszállíthatják. Minden más esetben eszközt kiszállítani csak a rendszergazda írásos engedélyével lehet. A ki- és beszállítások ellenőrzése a rendszergazda feladata. Infokommunikációs eszközök és berendezések írásos engedély nélküli ki- és beszállításának kísérlete esetét jelenteni kell az IBFnek a szabálysértést elkövető személy felettes vezetőjének egyidejű értesítése mellett.

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

9.3. Fizikai belépési engedélyek

A Hivatalnak össze kell állítania azon személyek listáját, akik jogosultak a védett és az érzékeny területekre történő belépésre. A listát a jegyző hagyja jóvá. Az IBF háromhavonta felülvizsgálja a belépésre jogosult személyek listáját és eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése már nem indokolt.

10. Humán erőforrás az ASP-ben

Az ASP rendszereket használó szervezeti egység vezetőjének a felelőssége, hogy meghatározza az egyes, ASP szakrendszer munkakörökhöz tartozó felelősségeket és feladatokat.

Alkalmasság vizsgálat:

- A Közös Önkormányzati Hivatal jegyzőjének a felelőssége, hogy foglalkoztatás előtt a betöltendő ASP rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelőségi vizsgálatot végezzen el a foglalkoztatni kívánt munkatárs vonatkozásában.
- A kockázattal arányos mértékben mérlegelni kell a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség stb.).
- Meg kell győződni arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.
- Az információbiztonsági szakterület vezetőjének felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására

kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.

- A jegyző felelőssége, hogy a foglalkoztatás alkalmával az önkormányzati hivatal munkaköri leírásban rögzítse a kockázatokkal arányosan a titoktartás követelményeit (ASP titoktartási nyilatkozat, mely korábban megküldésre került) és a foglalkoztatás egyéb kikötéseit.
- A jegyző felelőssége, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

11. Oktatás, képzés az ASP-ben

A Hivatal elektronikus információs rendszereit csak olyan személyek használhatják, akik megfelelő informatikai és számítástechnikai ismeretekkel rendelkeznek.
Rendszeres továbbképzésekkel és belső oktatásokkal gondoskodni kell arról. hogy a felhasználók az alapvető információbiztonsági ismeretekkel rendelkezzenek.

A Közös Hivatal munkatársaknak ASP oktatáson kell részt venni, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják. Az informatikai biztonsági képzés megszervezése az IBF feladata. Az oktatás folyamatát a képzési tervben kell rögzíteni. A képzési terveket évente a tárgyév január 31-ig készítjük el. A Hatóság és a Magyar Államkincstár a képzési terveket ellenőrizheti.

12. ASP jogosultság kezelés

A szerződésben meghatározott tenant adminisztrátorok rendszerbe történő „felvitelét" az ASP Központ végzi el az önkormányzat által megküldött adatlap alapján.

- A privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot osztanak. Ezt a tevékenységet az önkormányzati jegyző felelősségi és hatáskörébe tartozóan tudják elvégezni.
- Egy önkormányzati fióknál (tenantnál) minimum egy felhasználó karbantartónak szükséges „lenni", ezt a rendszer figyeli (pl.: nem lehet zárolni, vagy elvenni tőle a jogot, ha csak egyedüli felhasználó karbantartó a tenantnál).
- A rendszer használata során elvárt, hogy a privilegizált joggal rendelkező munkatársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használják.
- A privilegizált joghoz tartozó bejelentkezési azonosítót zárt borítékban, biztonságosan zárható helyen kell tárolni.

A tenant adminisztrátor feladatai:

- új felhasználók (userek) rögzítése,
- meglévő felhasználók adatainak módosítása,

- felhasználók zárolása (szükség szerint),
- felhasználói jogosultságok (szerepkörök) kiosztása,
- felhasználói jogosultságok módosítása, megvonása,
- helyettesítések beállítása, eltávolítása,
- felhasználói csoportok létrehozása, módosítása, törlése (ugyanazon szerepkörök kiosztása több felhasználónak),
- üzleti napló megtekintése (a rendszerben történő változásokat lehet lekérdezni, követni).

13. ASP rendszerbe történő belépés, authentikáció

A Belügyminisztérium – az Igazságügyi Minisztérium és a Nemzeti Adatvédelmi és Információszabadság hatóság bevonásával – megvizsgálta azt a kérdést, hogy az elektronikus személyi igazolvány (eSZIG) felhasználása az ASP rendszerbe történő azonosításra ütközik-e valamely jogszabályba, illetve szükséges-e az önkormányzat alkalmazásában álló közszolgálati tisztviselők jogszabályi kötelezése az eSZIG kiváltására. Ez nem ütközik jogszabályba.
Az ASP elsődleges autentikációs eszköze az eSZIG. A használatához javasolt kártyaolvasók hatóság által bevizsgált és elfogadott eszközök.
Az ASP eSZIG-gel történő azonosítás során személyes adathoz az ASP rendszer nem fér hozzá. Belépéskor ugyanis az e-személyi érvényességét közvetlenül a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalának (a továbbiakban: KEKKH) szervere ellenőrzi. A KEKKH szervere az ASP rendszernek egy ún. hash-kódot (RID) ad vissza, mely azonos okmány esetén mindig ugyanaz, de ez a kód nem fejthető vissza személyes adattá. Az ASP rendszer ehhez az anonim hash-kódhoz rendeli a felhasználót.
Az elektronikus személyigazolvánnyal történő authentikáció során a következő szabályzókra kell megkülönböztetett módon figyelni:

- Minden ASP rendszert használó munkatársnak rendelkeznie kell eSZIG-el.
- Az eSZIG használatához szükséges a kártyaolvasó számítógépre történő telepítése.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rögzített felhasználói fiók és az eSZIG összerendelése szükséges.
- A személyi igazolvány kártyát csak a tulajdonosa használhatja, azt ASP rendszer authentikációs folyamat céljából másnak átadni tilos.
- Az hivatal vezetőjének a jegyzőnek gondoskodnia kell arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen. Az ehhez tartozó szabályrendszer kialakítása elengedhetetlen.

14. Csatlakozó önkormányzat kliens oldali biztonsága

Az ASP kapcsán kiemelten kezeljük a biztonsági kockázatokat.
Fontos az ASP rendszerbe olyan kikerülhetetlen biztonsági megoldásokat beépíteni, ami szűkíti a felhasználók biztonságra kockázatos tevékenységének lehetőségét.

A lehetséges fenyegetettségek, sebezhetőségek, valamint ezek megelőzésére alkalmazható intézkedések az alábbiak pl.:

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

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

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	Hiányos biztonsági naplózás. A biztonsági naplók értékelésének elmulasztása vagy rendszertelensége.	Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.

14. 1. Munkaállomásokra vonatkozó biztonsági elvárások

Az ASP rendszerhez csatlakozó eszközök karbantartásáról, változáskövetéséről gondoskodunk a következők figyelembevételével:

- Biztosítjuk, hogy minden munkaállomásokon legyen telepítve vírusvédelmi program, a legfrissebb vírus definíciós adatállománnyal. A végpontvédelem tartalmazzon e-mail (csatolmány) védelmet is.
- A munkaállomásokon megoldott a böngésző megfelelő biztonsági beállítása.
- A tervszerű beavatkozásokhoz karbantartási időablakot jelölünk ki.
- A munkaállomások programfrissítését szükség szerint, de legalább havonta biztosítjuk, különös tekintettel a legfrissebben kiadott security patch komponensekre.
- Biztosítjuk, hogy a telepítő programok, a licensz azonosítók, zárható és tűzbiztos lemezszekrényben legyenek tárolva.

A munkaállomások elhelyezésénél biztosítjuk:

- A készülékek olyan módon legyenek a hivatalban elhelyezve, hogy azokat az ügyfelek ne tudják elérni.
- A monitor kijelzési képét az ügyfelek ne tudják elolvasni.
- Ideiglenesen magára hagyott készülékek zárolása, képernyővédő aktiválása.
- Munkaidő végén a munkaállomások kikapcsolása történjen meg.

Az ASP központhoz csatlakoztatott infrastruktúra elemekre biztosítjuk:

- A naplóinformációnak a védelmét,
- Hiba esetén a naplóbejegyzések elemzését,
- A rendszer hozzáférés ellenőrzését.

14.2. Hálózatbiztonság

A rendszer üzemeltetésével kapcsolatos elvárások:

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra. Legyen megoldott az azonosítók zárt borítékban, és biztonságosan zárható helyen történő tárolása. Csak előre kijelölt, privilegizált felhasználóknak legyen lehetősége bejelentkezni a kérdéses eszközökbe.
- A hálózati végpontok védelme legyen megoldva. A lehetőségek figyelembevétele mellett pl. port security, esetleg 802.1x szabványnak megfelelően.
- Az eszközök hálózatba történő illesztéséről készüljön dokumentáció.
- Az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történjen meg.
- A menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva.

14.3. Informatikai határvédelem, tűzfal

- A szervezet internethez való csatlakozástatása a központi tűzfalon keresztül történjen meg.
- A tűzfal szabályok dokumentálása és azok zárható helyen történő tárolása legyen biztosítva.

A tűzfal szabályok módosítása a kijelölt felelős előzetes, írásbeli engedélye alapján történhessen meg.

14.4. Emberi erőforrások biztonsága

A hozzáférési jogokat nyert felhasználók neveit és jelszavait minősítetten kell kezelni. Az azonosítás és hitelesítés folyamatainak meg kell előznie az információs rendszerrel kapcsolatos bármilyen más engedélyezett beavatkozást. A kliens-szerver alkalmazásoknál az azonosításnak és a hitelesítésnek mind a kliens, mind a szerver oldalon meg kell történnie.
A hozzáférési jogosultságokat folyamatosan aktualizálni kell.
A felhasználói azonosítást egyértelműen kell hozzárendelni minden egyes személyhez, azaz nem létezhet több személy azonos, közös jelöléssel.
Ki kell dolgozni a hozzáférési jogok nyilvántartási rendszerét, amely rendszerenként, szerepkörönként, személyenként tartalmazza a szükséges adatokat. A hivataltól távozó alkalmazottak hozzáférési jogait inaktívvá kell tenni.
Biztosítani kell a jogosultság nyilvántartás folyamatos és naprakész vezetését.
Biztosítani kell, hogy az operációs rendszer rendelkezzen megfelelő hozzáférés-ellenőrzési funkciókkal.

A felhasználóknak ismerniük kell a jelszavak, illetve a kezelésükben lévő berendezések használatára vonatkozó előírásokat. A jelszót a felhasználó semmilyen körülmények között nem jelenítheti meg különböző adathordozókon, képernyőn, papíron stb. A jogosulatlan hozzáférés kísérlete esetén a felhasználót felelősség terheli, amit jelenteni kell a jegyzőnek.

A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket. A Hivatal elektronikus rendszereit csak az APS titoktartási nyilatkozat aláírása után lehet használatba venni.

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

- Hozzáférési jogosultságok megszüntetése
- A használatra átvett informatikai eszközök visszaszolgáltatása

A biztonsági előírások megsértőjével szemben fegyelmi felelősségre vonásra kerülhet sor.

14.5. Külső szolgáltatókkal kapcsolatos előírások

Külső üzleti partner csak meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal, amit szerződésben kell dokumentálni. A külső üzleti partner hozzáférése a Hivatal adataihoz csak a titoktartási nyilatkozat aláírása után lehetséges.

15. Jelentés a biztonsági eseményekről

A biztonságot érintő gyenge pontokról, szoftverzavarokról, rendkívüli IT biztonsági eseményekről a felfedezést követően azonnal értesíteni kell a jegyzőt és az információbiztonsági felelőst.

Mit is értünk rendkívüli IT biztonsági esemény (IT biztonsági incidens) alatt? Az informatikai rendszer védelmi állapotában beállt illetéktelen változás, amelynek hatására az informatikai rendszerben kezelt információ bizalmassága, sértetlensége, hitelessége, funkcionalitása, rendelkezésre állása megsérül, vagy a sérülésük kockázata megnő. Ilyen esemény lehet például adathalászok támadása, eszközök, adathordozók eltulajdonítása stb.

Amennyiben a biztonságot érintő esemény érinti az önkormányzati ASP rendszer által nyújtott szolgáltatásokat, vagy közvetlenül azokban következik be, az eseményt írásban jelenteni szükséges az ASP rendszer működtetőjének is.

A jelentésben rögzíteni szükséges:

A biztonsági esemény megnevezése, helye, időpontja, leírása, észlelő neve, a kivizsgálás eredménye, a megtett intézkedés leírása. A jelentés elkészítéséhez a jelen szabályzat mellékletében található iratmintát használjuk.

Az információbiztonsági felelős a bejelentett biztonságot érintő eseményekről, veszélyes helyzetekről, működési zavarokról, azok előfordulási gyakoriságáról, a kezelésükre tett intézkedések eredményéről háromhavonta beszámol a jegyzőnek.

Szükség esetén soron kívül is jelentést tesz a jegyző részére.

Az információbiztonsági felelős feladata az események kezelése során nyert tapasztalatok alapján a meglévő biztonsági rendszer fejlesztésére történő javaslat készítése.

16. Kockázatelemzés és kezelés

Az információbiztonsági kockázatelemzés célja, hogy feltárja a Hivatal elektronikus információs rendszereire és az azokban kezelt adatokra ható fenyegető tényezőket, veszélyforrásokat, vizsgálja a rendszer gyenge pontjait, elemezze a veszélyforrások által a gyenge pontokon bekövetkező sikeres támadások bekövetkezésének valószínűségét, az általuk várható kár nagyságát, valamint kezelje a kockázatokat.

A kockázatarányos védelem kialakításához rendszeres és tervszerű informatikai kockázatelemzésre van szükség.

Szervezetünknél az információbiztonsági kockázatelelemzést évente tárgyév március 31-ig az információbiztonsági felelős köteles elvégezni.

Soron kívüli kockázatelemzést végzünk, ha változás áll be az elektronikus információs rendszerben, új fenyegetések jelennek meg.

16.1. Információs kockázatkezelés és megfelelés az előírásoknak

Az információs rendszereket veszélyeztető kockázatokat olyan módon kell kezelni, hogy azt a jogszabályok által előírt és a szervezet vezetője által elfogadott szinten tartsuk.
Az információs vagyonelemek értékelésére és biztonsági osztályba sorolására folyamatokat kell kialakítani, azért, hogy a vagyonelemeknek az értéküknek megfelelő védelmet biztosítsuk.
Meg kell határozni az információs rendszerekkel kapcsolatos összes elvárást (jogszabályi, hatósági, tulajdonosi, szerződéses és más követelmények), ezért hogy a követelmények nem teljesítésének kockázatát kezelhessük.
Rendszeresen el kell végezni a sérülékenységek, fenyegetések felmérését az információt fenyegető kockázatok azonosítása érdekében. A kockázatvállalási szintnek megfelelő kockázatkezelési intézkedéseket kell alkalmazni.
Értékelni kell az információbiztonsági kontrollokat, hogy megfelelőek-e a kockázatok csökkentésére, és ténylegesen megfelelően működnek-e.
A jelenlegi kockázati szint és az elvárt kockázati szint közötti különbséget meg kell határozni.
Az információbiztonsági kockázatok kezelésének tevékenységeit be kell építeni a szervezet minden működési folyamatába annak érdekében, hogy egységes legyen a kockázatok kezelése.
Folyamatosan figyelemmel kell kísérni a kockázatoknak, és a kockázatok mértékének a változását, hogy megfelelően kezelhessék őket.
A szervezet megfelelő szintjén lévő vezetőket tájékoztatni kell a kockázatok változásáról, és a követelmények esetleges sérüléséről azért, hogy megalapozott döntéseket hozhassanak.

16.2. Információbiztonsági program kidolgozása és megvalósítása

Az információbiztonsági programot az információbiztonsági stratégiával összhangban kell kialakítani és megvalósítani.
Biztosítani kell az információbiztonsági program információbiztonsági stratégiával való összhangját.
Az integráltság növelése érdekében a szervezet alap- és működési folyamataihoz illeszkedve kell az információbiztonsági programot megvalósítani.
Az információbiztonsági program végrehajtásához szükséges belső és külső erőforrásokat azonosítani, rendelkezésre állásokat pedig biztosítani és menedzselni kell. Az információbiztonsági program végrehajtásának megfelelő információbiztonsági architektúrát (emberek, folyamatok, műszaki megoldások) ki kell alakítani és fenn kell tartani.

A szervezet információbiztonsági szabványait, eljárásait, útmutatóit és más, vonatkozó dokumentumokat az információbiztonsági politikának megfelelően kell kialakítani, kommunikálni és karbantartani.
A biztonságos környezet, és a ténylegesen biztonságtudatos szervezeti kultúra elősegítésére információbiztonság-tudatosítási programot és képzési rendszert kell kialakítani és fenntartani.
A szervezet alapvető biztonsági szintjének fenntartása érdekében az információbiztonságból fakadó követelményeket bele kell építeni a szervezet folyamataiba (pl.: változtatások felügyelete, katasztrófa helyreállítás, stb.).
A szervezet alapvető biztonsági szintjének fenntartása érdekében a harmadik felekkel (pl. informatikai szolgáltató, takarító cég) kötendő szerződésekbe be kell építeni az információbiztonsági követelményeket.
Az információbiztonsági program eredményességének és hatékonyságának értékelésé érdekében meg kell teremteni a program végrehajtásának feltételeit és ki kell dolgozni a működést mérő mutatószám rendszert. A mutatószámok alakulását figyelemmel kell kísérni, és a vezetés számára időszakonként jelentéseket kell készíteni.

16.3. Információbiztonsági kockázatok

Az információbiztonság szempontjából kockázat alatt az adott információs rendszer, vagy az információ fenyegetettségének mértékét értjük. A kockázat elemzés során fel kell tárni a rendszerek gyenge pontjai (sebezhetőség) és az azt érő fenyegetéseket, majd meg kell határozni a bekövetkezés valószínűségét és a várható kárát. Az információs rendszer sebezhetősége a rendszer tervezésének, megvalósításának, vagy működésének olyan gyengesége, amely a rendszer elleni támadás során kihasználható, és emiatt fennáll a biztonság sérülésének lehetősége. Az információs rendszer szempontjából fenyegetésnek tekintünk minden olyan körülményt vagy eseményt, amely az adatok, vagy információs rendszerek biztonságát fenyegethetik. Ide soroljuk például a személyektől eredő támadásokat (pl. számítógépes betörés), és a külső behatásokat (pl. földrengés).

A közigazgatási információs rendszerek működésében tapasztalt tipikus biztonsági kockázatok:
• egy új rendszer a beüzemelést követő néhány héten belül több napra megbénul;
• vezető munkatársak adathordozói illetéktelenek kezébe kerülnek a rajta levő személyes levelezéssel, nem nyilvános adatokkal;
• a munkájában el nem ismert rendszergazda az üzemeltetési feladatok naprakész pontos dokumentálása nélkül távozik;
• a munkatársak áthelyezésüket követően is hozzáférnek a korábbi szervezeti egységük anyagaihoz.

Mi okozza a biztonsági kockázatok növekedését:
• az informatikai szolgáltatásoktól és az adatkapcsolat folyamatosságától való függés;
• a szándékos károkozás megnövekedett motivációja;
• a nagy informatikai beruházást is tartalmazó projektek kudarcai;
• a hardver, illetve szoftver eszközök meghibásodása;
• a virtuális vállalatok terjedése;
• az időjárás változása.

Az információbiztonsági kockázatok kezelésének négy alapmódszere van:
• a tevékenységek beszüntetése (kockázat megszűnik);
• a tevékenység kockázataira biztosítás kötése (kockázatot áthárítottuk a biztosítóra);
• a felelős vezető a kockázatot megismeri és nem tart további intézkedést szükségesnek (kockázatot a szervezet felvállalta);
• a felelős vezető védelmi intézkedéseket (kontroll) valósít meg, vagy szüntet meg (kockázati válasz meghatározása és megvalósítása).

Akkor tekintjük jónak a védelmi rendszert, ha egy kellően nagy időintervallumon belül – ami jellemző a szervezet tevékenységére – a kockázatok csökkentésére fordított költségek (védelem) arányosak a kockázat bekövetkezéséből fakadó várható kár mértékével.

16.4. Megfelelés az előírásoknak

Megfelelés (compliance) alatt a közigazgatási szervezetek kötelezettségei bemutatásának, és a kötelezettségteljesítés bemutatásának képességét értjük, amely által a jogszabályi, hatósági, belső szabályozásból fakadó, illetve a szerződéses előírásokat, elvárásokat folyamatosan teljesíti.

A követelmények azonosítása és a megfelelés biztosítása a belső védelmi vonalak részét képező belső kontroll funkció, amely elősegíti a szervezet prudens, megbízható az előírásoknak megfelelő működését. Feladata a megfelelőséget veszélyeztető kockázatok azonosítása és kezelése. Az előírásoknak megfelelés érdekében az összes szakterületnek együtt kell működnie az alábbi tevékenységek végrehajtásában.

• megfelelőségi kockázatok meghatározása; mérése, kontrollkörnyezet értékelése;
• megfelelőségi program tervezése és megalkotása (felülvizsgálata);
• szervezet megfelelőségi tevékenységének figyelemmel kísérése;
• felügyeleti és hatósági kapcsolattartás;
• tanácsadás a felső vezetés számára;
• munkatársak képzése;
• pénzmosás és csalás megelőzés;
• összeférhetetlenség kezelése.

16.5. Biztonsági szabályozási és kontroll rendszer

A kontroll rendszer megvalósítása során, a kockázatok ismeretében három alapvető kontroll típus kombinációját kell alkalmazni:
• megelőző kontroll: olyan ellenőrzési eljárás, amely megelőzi, vagy korlátozza egy hiba bekövetkezését, mint például a fizikai hozzáférés megakadályozása, vagy a szoftverek jogosultságainak korlátozása;
• feltáró kontroll: olyan ellenőrzési eljárás, amely lehetőség szerint mielőbb feltárja a bekövetkezett hibákat, hiányosságot, mint például az ellenőrző összeg a számítási műveleteknél;
• helyesbítő kontroll: olyan ellenőrzési eljárás, amely a bekövetkezett hibákat, hiányosságokat segít megszüntetni, hatásukat csökkenteni , az informatikai katasztrófa-helyreállítási terv alapján.

A kontroll rendszer tervezése során minden tevékenységben rejlő kockázatot (benne rejlő kockázat) a szervezet vezetője által elfogadhatónak tartott szintre kell csökkenteni.

16.6. Biztonsági monitoring

A telepítés pillanatában ismert és elvárható biztonsági beállítások elvégzését a rendszer telepítőjétől kell elvárni, azonban önmagában ez nem nyújt sokáig védelmet. A védelmi rendszerbe folyamatosan be kell illeszteni az újonnan megjelenő védelmi szolgáltatásokat és intézkedni kell a felmerülő kockázatok kezeléséről. Általában a gyakorlatban a biztonságot annak hiányával mérjük, az adott időszakban bekövetkezett rendkívüli információbiztonsági események száma megmutatja, hány alkalommal sérülhetett a biztonság. A feltárt belső visszaélések száma jó mutató lehet az etikus és biztonságtudatos magatartás szintjének megítéléséhez. Ezek a mutatók azonban nem tekinthetők objektívnek. A rendkívüli események számát befolyásolja például, hogy milyen az ellenőrzési rendszerünk megbízhatósága, azaz, ha magas színvonalú a hálózatfelügyeleti rendszerünk, akkor észreveszünk minden lényeges biztonsági eseményt, ezáltal a feltárt biztonsági események száma megnő, de a biztonság kevésbé sérül. Ugyancsak befolyásolja a nyilvántartott biztonsági események számát, hogy minden eseményt bevezetnek-e a nyilvántartásba. A cél az, hogy mind a rendszerek működését, mind a bekövetkezett biztonsági eseményeket figyelemmel kísérjük. Erre egyrészt a hagyományos rendszer- és hálózatfelügyeleti szoftverek használata, másrészt a biztonsági események elemzéséhez központi naplógyűjtő rendszer és naplóelemzési jelentések kialakítása szükséges, amely a lényeges kockázatok szoros felügyeletét teszi lehetővé. A fejlett biztonsági monitoring része ma már az automatikus sérülékenység vizsgáló eszközök alkalmazása, amelyek segítik a rendszerek naprakész frissítését, és javaslatot tesznek a szükséges változtatások telepítésére. Új rendszerek bevezetésének tervezésekor nem szabad elfelejtkezni a biztonsági kontroll és monitoring funkciók szükségességétől.

17. Kockázatelemzési és kezelési módszertan

17.1.Vagyonleltár

Az elektronikus információs rendszerekre ható fenyegetettségek különbözőek, attól függően, hogy az elektronikus információs rendszer melyik összetevőjét fenyegetik. A fenyegetettségek megfelelő azonosítása érdekében a létre kell hozni és értelemszerűen fel kell mérni a következő vagyonelem csoportokat

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

17.2.Helyzetfelmérés

Az információbiztonsági kockázatelemzés elvégzéséhez fel kell mérni, meg kell ismerni az elektronikus információs rendszereket és azok környezetét, valamint azok jelenlegi információbiztonsági szintjét. A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

I. Adminisztratív védelmi intézkedések

- A Hivatalra vonatkozó jogszabályok, szabályzatok
- Az elektronikus információs rendszerre vonatkozó szabályzatok
- Szerződések, külső felek kezelése
- Alkalmazásfejlesztés, változáskezelés
- Jogosultságigénylés
- Biztonsági események kezelése
- Üzemeltetési eljárások
- Szervizelés, eszközcsere, selejtezés

II. Logikai védelmi intézkedések

- Mentési megoldások
- Kártékony kód elleni védekezés
- Biztonsági frissítések telepítése
- Hálózat felépítés
- Biztonsági rendszerek
- Kriptográfiai megoldások

III. Fizikai biztonság

- Beléptetés
- Számítógépterem kialakítása
- Épületben történő közlekedés
- Irodák kialakítása, tiszta asztal, üres képernyő politika

17.3. Gyenge pontok meghatározása

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

17.4. Fenyegetettségek elemzése

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

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

17.5. Sérülékenységek elemzése

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

Kárérték szintek kialakítása, károk rávetítése a vagyonelemekre

A következő kárérték szintek kerültek meghatározásra:

Kárérték szint	Kár leírása
1	Jelentéktelen kár
2	Egy adott szakrendszer sérül
3	Több szakrendszer sérül
4	Valamennyi szakrendszer sérül

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

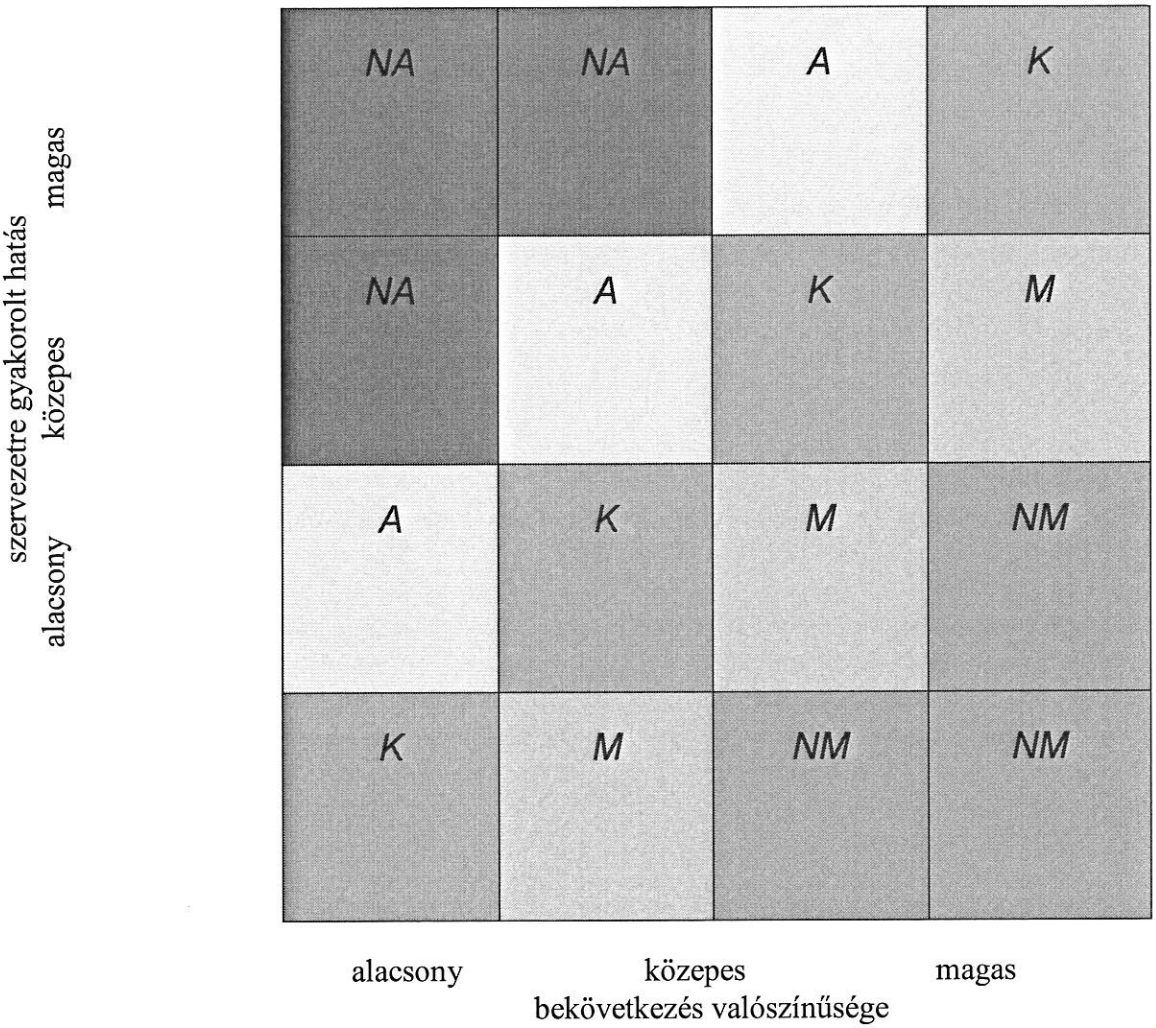
A bekövetkezési valószínűségek meghatározása

Következő lépésként meg kell becsülni a sérülékenységek bekövetkezési valószínűségét.
A bekövetkezési valószínűséghez a következő értékeket kell használni:
- 4 - bármikor bekövetkezhet
- 3 - gyakori
- 2 - közepes
- 1- ritka

17.6. Kockázatok meghatározása

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

A kockázatok minősítéséhez a következő kockázati mátrixot kell definiálni:



A kockázatok jelölése a következő:

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

Elviselhető kockázatok meghatározása

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

szervezetre gyakorolt hatás				
magas	T	T	T	EV
közepes	T	T	EV	NT
alacsony	T	EV	NT	NT
	EV	NT	NT	NT
	alacsony	közepes		magas

bekövetkezés valószínűsége

A táblázatban alkalmazott jelölések értelmezése a következő:
- T – Tolerálható
- NT – Nem tolerálható
- EV – Egyenként vizsgálandó

Kockázatok kezelése
A nem tolerálható kockázatokat kezelni kell.
A Hivatal a kockázatokat a következőképpen kezeli:
a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (Kockázat csökkentés);
b) Tudatosan, a következményeket felmérve elfogadja a kockázatot (Kockázat elfogadás);
c) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (Kockázat elkerülés);
d) Áthárítja a kockázatot például biztosítással, vagy megfelelő beszállítói szerződésekkel. (Kockázat áthárítás).

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

Kockázatcsökkentő intézkedések
A PreDeCo elv alapján a kockázatcsökkentés három szemszögből közelíthető meg:
a) Megelőző jellegű (preventív kontrollok) A hibák, gyengeségek, sérülékenységek, illetve ezek kihasználására való lehetőségek kiküszöbölése.
b) Korlátozó vagy javító (korrektív kontrollok) Egy veszély hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.
c) Észlelő és reagáló (detektív kontrollok) A sebezhetőségek támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

17.7. Kockázatok és intézkedések nyilvántartása

Szervezetünknél a kockázatelemzést és annak értékelését minden év március 31-ig kell elvégezni, amelynek a felelőse az információbiztonsági felelős. A kockázatokról és az intézkedésekről nyilvántartást kell vezetni. A nyilvántartás céljára a szabályzat mellékletében található iratminta szolgál.

18. Nemzeti Elektronikus Információbiztonsági Hatóság

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. Korm. határozata meghatározta Magyarország kibertérre vonatkozó értékrendjét, jövőképét és céljait, és előre vetette a dinamikusan változó kibertér igényeihez és az ez által generált feladatokhoz alkalmazkodni képes kormányzati képességeket biztosító kormányzati struktúra kiépítését. A stratégia gyakorlati megvalósulását hivatott biztosítani még a 2013 áprilisában elfogadott, az állami és önkormányzati rendszerek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv). A törvény felállítja a szükséges intézményrendszert a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága alapfeltételei megteremtéséhez. Az intézményrendszer része a Nemzeti Biztonsági Felügyelet új szakhatósági feladata, amely

keretében a biztonsági incidensek megelőzését, a sérülékenységek és hibás működési beállítások felkutatását végzi, továbbá javaslatot tesz azok elhárítására, valamint közreműködik a biztonsági incidensek műszaki vizsgálatában. Az Ibtv. és végrehajtási rendeletei létrehozták a Nemzeti Elektronikus Információbiztonsági Hatóságot (továbbiakban: NEIH) és szakhatósági feladatokkal ellátásával ruházzák fel az elektronikus információbiztonság területén. A Hatóság fő feladata, hogy felügyelje a költségvetési szervek információtechnológiai, adatkezelő- és feldolgozó tevékenységét és az információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülését. Továbbá engedélyezi az érintett szervezetek által az Európai Unió tagállamaiban történő elektronikus információs rendszer üzemeltetését, és ellenőrzi az érintett szervezetek által az Európai Unió tagállamain kívül történő elektronikus információs rendszerüzemeltetést.

A Nemzeti Elektronikus Információbiztonsági Hatóság feladatait és hatáskörét a 301/2013. (VII. 29.) Kormányrendelet rögzíti.
Címe: 1440 Bp., Pf.: 1.

A hatóság nyilvántartja és kezeli:

- a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,
- a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, a 13. § (8) bekezdésében meghatározott végzettségét,
- a szervezet informatikai biztonsági szabályzatát,
- a biztonsági eseményekkel kapcsolatos bejelentéseket.

A hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult:
az érintett szervezeteknél a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,

A szervezet informatikai biztonsági szabályzatát, valamint a biztonsági felelős természetes személy azonosító adatait, telefon és fax számát, e-mail címét, végzettségi adatait a NEIH részére 2014. február 5-ig meg kellett küldeni. Az adatváltozásokat 8 napon belül kell közölni a hatóság részére.
Az adatközlés felelőse szervezetünknél a jegyző.

II.
KONFIGURÁCIÓ KEZELÉSI ELJÁRÁSREND

1. Alap konfiguráció

A Hivatal valamennyi elektronikus információs rendszeréhez el kell készíti az alapkonfigurációt, amelyet dokumentált formában biztonságos helyen tárolni szükséges. A dokumentációnak minimálisan a következő elemeket kell magában foglalnia:
a) Hardver elemek;
b) Szoftverek;
c) Telepítőkészletek;
d) Egyes szoftverkomponensek alapkonfigurációi.

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

2. Elektronikus információs rendszerelem leltár

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

3. Szoftver használat korlátozásai

A Hivatalban kizárólag a jegyző által engedélyezett, jogtiszta, a megfelelő licence-el rendelkező szoftvereket lehet használni. Az alkalmazott szoftverekről leltárt kell vezetni. Szabad vagy nyílt forráskódú szoftverek használatbavételét a jegyző engedélyezi. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell. A másolatok és szétosztások ellenőrzése érdekében a telepítőkészleteket és a licenceket tartalmazó dokumentumokat páncélszekrényben kell tárolni és a hozzáféréseket ellenőrizni kell. A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni. A felhasználók semmilyen alkalmazást nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a kiszolgálókra és munkaállomásokra csak a rendszergazda végezheti el. A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróbaszerűen ellenőrzi.

4. Ügymenet folytonosság

A Hivatal elektronikus információs rendszereinek folyamatos működésének biztosítása érdekében, valamint a katasztrófa-helyzetek bekövetkezte során a jelen fejezetben foglaltak szerint kell eljárni. Az önkormányzati ASP rendszer által nyújtott szolgáltatások üzletmenet folytonosságának a biztosítása a működtető feladata. Ügymenet folytonosságra vonatkozó eljárásrend Az IBF-nek az érintett területek bevonásával ki kell dolgoznia és jóvá kell

hagyatnia az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet (továbbiakban: ÜFT). A folyamatos működés tervezésére vonatkozó tevékenységeket össze kell hangolni a biztonsági események és vészhelyzeti/katasztrófa helyzetek kezelésével. A tervezés során meg kell határozni a Hivatal által biztosítandó szolgáltatásokat és alapfunkciókat, valamint az ezekhez kapcsolódó és a Hivatal részéről elvárt vészhelyzeti követelményeket. Meg kell határozni az elektronikus információs rendszer kiesése esetére a helyreállítási feladatokat, a helyreállítási prioritásokat és azok mértékét. Ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket. Az ügymenet-folytonosságot úgy kell kialakítani, hogy az biztosítsa a Hivatal által előzetesen definiált alapszolgáltatások fenntartását, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is. Ki kell dolgozni a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

Az Ügymenet-folytonossági tervet évente felül kell vizsgálni.

Az Ügymenet-folytonossági tervet soron kívül felül kell vizsgálni
a) az elektronikus információs rendszer vagy a működtetési környezet jelentős változása,
b) az ügymenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémák esetén.

Az Ügymenet-folytonossági terv változásairól képzés formájában tájékoztatni kell a felhasználókat.

5. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jogszabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárásrendet kell kidolgozni a következők figyelembevételével:
Rendszeres mentéseket kell készíteni a legalább 2-es biztonsági osztályba sorolt elektronikus információs rendszerekről és az azokban kezelt adatokról.

A mentések során a következő adatfajták mentését kell biztosítani:
a) felhasználói szintű adatok (ügyviteli adatok)
b) rendszerszintű információk
c) a rendszerrel kapcsolatos dokumentációk.

Biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a lényeges adatok és szoftverek esetleges adathordozó hiba, az elektronikus információs rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek. A mentési eljárásrendet úgy kell kialakítani, hogy az egyrészt megfeleljen az üzembiztonsági elvárásoknak, másrészt minél biztonságosabb védelmet nyújtson az esetlegesen előforduló hibák ellen. Az alkalmazások fizikai védelme érdekében, gondoskodni kell arról, hogy a telepítő állományok ne károsodjanak, ezért az eredeti példányukról biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tárolni. Az eredeti hordozókról készített másolatokat kell a napi tevékenység során használni. Az olvasási

biztonság fenntartása érdekében az eredeti adathordozókról rendszeres időközönként frissítő mentést kell készíteni.

6. Az elektronikus információs rendszer helyreállítása és újraindítása

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

- katasztrófát követő helyreállítandó célállapot;
- a katasztrófa események definíciója;
- a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;
- a helyreállítási terv hatóköre;
- a megelőzés érdekében végzett tevékenységeket;
- felkészülés a katasztrófa elhárítására;
- katasztrófa esetén végrehajtandó tevékenységek;
- elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot;
- a helyreállítási terv tesztelése, karbantartása.

Az elektronikus információs rendszerekre vonatkozó helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terv készítési tevékenységeket az IBF-nek információbiztonsági szempontból támogatnia és rendszeresen ellenőriznie kell. A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása). A rendszergazdának - mindezeken túl - gondoskodnia kell az elektronikus információs rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.

6. 1. Vészhelyzetek

Minden megelőző intézkedés dacára előfordulhatnak vészhelyzetek:

- **Hardverhiba:** A merevlemezeknél is felmerülhet időnként mechanikus hiba (hiszen végső soron mozgó elemekből állnak), rossz szektor jöhet létre, vagy elromolhat valamelyik elektromos alkatrész.
- **Szoftverhiba:** Alkalmazáshiba, az operációs rendszer összeomlása vagy torlódás (lockup) is károsíthatja az adatokat. Rosszindulatú számítógépes vírusok okozta adatvesztés.
- **Természeti katasztrófák:** A számítógép elemeinek (és a rajta tárolt adatoknak) általában nincs túl sok esélyük a természeti csapásokkal (tűz, árvíz, áramkimaradás) szemben.
- **Emberi hiba:** Emberi mulasztás véletlenül megváltoztathatjuk vagy letörölhetjük a számunkra fontos adatokat.

Ilyen esetekben négy fontos célt kell szem előtt tartani:

- Lehetőség szerint előzzük meg a további károkat.
- Hozzunk megfelelő intézkedéseket a hasonló esetek elkerülésére.
- Segítsük elő a normál üzem visszaállását.
- Segítsük elő az okok kiderítését vagy a nyomozást.

6. 2. További károk megelőzése

Hardverhiba, vagy vétlen adatvesztés esetén hívjunk szakembert. Szoftverhiba esetén értesítsük a szoftver gyártóját vagy telepítőjét. A további károk megelőzésére a külső hálózati kapcsolatot szakítsuk meg. A belső hálózat particionálása történjen meg a támadás, vírusfertőzés továbbterjedésének megakadályozására. A védett rendszereket kapcsoljuk le. Természeti katasztrófák esetén a Szervezet ide vonatkozó szabályzatai (Tűzvédelmi, Munkavédelmi) szerint járjunk el.

Fontos arra figyelni, hogy megtaláljuk a kellő kompromisszumot a kár megelőzése és a rendszer ezen célú megállítása között, hiszen nem szerencsés, ha bármely vészhelyzetre azzal válaszolunk, hogy megszüntetjük rendszerünk működését. A megfelelő logikai zónák kialakításával a támadás súlyosságától függően van lehetőségünk arra, hogy milyen mértékben avatkozzunk be a rendszer működésébe.
Néha célszerű a támadásra úgy reagálni, hogy hagyjuk a támadást folyni, de közben, a támadó számára lehetőleg észrevétlenül, megfigyeljük tevékenységét. Ez segíthet a következő pont megvalósításában.

6. 3. Hasonló esetek megelőzése

Megtörtént eseményt követően nem elegendő az aktuális veszélyhelyzetet megszüntetni, pl. vírustámadás esetén a hálózati kapcsolat megszakításával, hiszen várható, hogy azon a módon, ahogy ez a támadó bejutott, más is be fog jutni. Meg kell keresni és be kell tömni a biztonsági rést! Ebben nagy segítségre lehet, ha megfigyeljük a támadás folyamatát, ugyanis ekkor könnyebben tudunk következtetni arra, hogy mi is volt az a tényező, amelyet kihasználva bejutott a támadó.

6. 4. Normál üzem visszaállítása

A normál üzem visszaállítása egy káresemény után igényli nem csak a sérült adatok visszaállítását, de a rendszer integritásáról való megbizonyosodást is. Erre célra különböző eszközök léteznek, amelyek a rendszer aktuális állapotát összehasonlítják valamely korábban elmentett állapottal (rendszerint ellenőrzőösszegek alapján).

Természetesen kétséges helyzetben legcélszerűbb a rendszer újratelepítése, ez azonban általában munkaigényes és nagy fennakadással áll. Célszerű lehet a telepített és felkonfigurált rendszerről egy „pillanatfelvételt" készíteni, amely lehet a merevelemez másolata Norton Ghost, programmal. Probléma esetén csak ezt a másolatot kell visszatölteni és visszaáll az eredeti állapot. Ez a megoldás kellő körültekintéssel használva nagyon gyors visszaállást tesz lehetővé, de nem szabad megfeledkezni a mentés óta történt változtatások (és biztonsági javítások!) feltöltéséről.

6. 5. A hiba okainak felderítése

Gyakori, hogy a normál üzem visszaállítása után szeretnénk kideríteni az okokat, vagy akár más lépésekre, pl. rendőrségi feljelentés is sor kerülhet. A fontosabb lépések:

- Készítsünk egy-az-egy másolatot a merevlemezekről! Erre alkalmas a Norton Ghost Windows alatt. Természetesen szükség van egy legalább akkora méretű lemezre, mint amelyről másolatot készítünk. A további vizsgálódást ezen a másolaton végezzük.
- Mentsük el, esetleg nyomtassuk ki a releváns napló állományokat! Gyakori, hogy a normál működés során a napló állományok előbb-utóbb felülíródnak, így a régebbiek elvesznek. Ezt meg kell akadályozni!
- Jegyezzünk fel minden fontos adatot (rendszerben futó programok, felhasználók, stb. listája.

7. Rendszer karbantartási eljárásrend

- Az elektronikus információs rendszerek karbantartására vonatkozóan a jelen fejezetben leírtak az irányadók. Az önkormányzati ASP rendszer szakrendszereinek rendszeres karbantartása a működtető feladata.

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

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

7. 1. A karbantartások dokumentálása és nyilvántartása

Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani.
A nyilvántartásba a következő adatokat kell minimálisan rögzíteni:
a) az elvégzett karbantartás megnevezése,
b) az érintett eszközök, szoftverek, elektronikus információs rendszerek,
c) a karbantartás engedélyezője,
d) a karbantartás elvégzője,
e) a karbantartás dátuma,
f) leállási idő (ha volt ilyen).
A jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz.
A karbantartások ütemezése Éves karbantartási tervet kell készíteni, melyben meg kell tervezni a karbantartások ütemezését. A terv elkészítése az információbiztonsági felelős,a terv jóváhagyása a jegyző feladata.

A karbantartás ellenőrzése
Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.
Karbantartási tevékenységet csak olyan külső fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte a Hivatal vonatkozó információbiztonsági előírásait.

A karbantartást végző külső felekről nyilvántartást kell vezetni, melynek minimálisan a következőket tartalmaznia:
a) szervezet megnevezése,
b) szerződésszám,
c) szerződés időtartama,
d) szerződéses kapcsolattartó neve, elérhetősége,
e) karbantartás végzők neve, elérhetősége,
f) szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

III.
ADATHORDOZÓK VÉDELME

1. Hozzáférés az adathordozókhoz, adathordozók használata

A Hivatalban csak a Hivatal tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtani.

Az adathordozók védelmére és azonosítására az adathordozókat azonosítóval (címkével) kell ellátni és azokról nyilvántartást kell vezetni. Az eszközhasználatot, a Hivatal elektronikus információs rendszereihez történő csatlakoztatása után, a Hivatal minden előzetes értesítés nélkül figyelheti, monitorozhatja. Otthoni munkavégzés és bármilyen más célból bármilyen adatot floppyn, CD-n, elektronikus levélben vagy egyéb más módon (Pl.: Pen drive) a Hivatal informatikai infrastruktúrájából kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának vagy a szervezeti egység vezetőének kell engedélyeznie, minden esetben írásos formában. A Hivatal az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

A mentést tartalmazó adathordozók megőrzési idejét úgy kell meghatározni, hogy azokról az aktuális adatállomány sérülés esetén visszaállítható legyen.

Vírust tartalmazó, nem mentesíthető adathordozót használatban tartani nem lehet.
Az adathordozót óvni kell a szennyeződésektől és a fizikai sérüléstől, használat után pedig zárható dobozban, vagy a gyári csomagolásban elektromos erőterektől távol (monitor, televízió, hangszóró, ventilátor, telefon, rádió, stb.) kell tartani.

Külső szervnek átadott adathordozókról bizonylatot (az átadás, átvétel időpontját, az átadás célját, az átadott adathordozó számát, tartalmát az átvevő szerv megnevezését és címét, az átadás idejét, (ideiglenesen vagy véglegesen) az átvevő szerv őrzéssel megbízott felelősének megnevezését, valamint az átadó és átvevő szerv erre feljogosított képviselőjének aláírását tartalmazó jegyzéket) kell készíteni.

2. Az adathordozók selejtezése

A szervezet által vásárolt és a dolgozó(k) részére kiadott adathordozót abban az esetben kell selejtezni, ha:

- fizikailag megsérült,
- gyári, gyártási hibából következően felhasználásra alkalmatlan,
- a tároló kapacitás a megengedhető érték alá csökken,
- véglegesen elhasználódott.

A felhasználók felelőssége, hogy a használhatatlanná vált adathordozókat (CD, DVD, stb.) a szervezet vezetője felé jelezze, aki gondoskodik azok közös helyen történő összegyűjtéséről. A selejtezés előtt biztosítani kell az adathordozón tárolt adatok biztonságos törlését (fizikai törléssel, formattálással). Ha a tárolt adatok biztonságosan nem törölhetők, akkor az adathordozót úgy kell megsemmisíteni, hogy további felhasználásra már alkalmatlan legyen, azaz fizikai roncsolással kell használhatatlanná tenni.

A megsemmisítés során a felesleges vagyontárgyak hasznosításának és selejtezésének szabályzatában előírtak szerint kell eljárni, annak tényét megsemmisítési jegyzőkönyvben kell rögzíteni.

3. Az infokommunikációs eszközök biztonsága

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

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

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;
b) cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;
c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek, emiatt nem szabad őrizetlenül hagyni autóban, szállodai szobában;
d) a mobil infokommunikációs eszközök ellopása esetén:

- az ellopás tényét a lehető leggyorsabban jelenteni kell az IBF-nek;
- értesíteni kell a rendőrséget;
- értesíteni kell a szálloda vezetését, ha az eszközt a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;
- valamennyi rendőrségi jelentést meg kell őrizni és a jegyző részére át kell adni.

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

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

4. Azonosítási és hitelesítési eljárásrend

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

Valamennyi elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie a Hivatal valamennyi felhasználóját és a felhasználók által végzett tevékenységeket.
Ennek érdekében egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat az információbiztonsági felelős hozza létre. Az azonosítók ismételt felhasználása tilos.
2 hónap inaktivitás után az azonosítókat le kell tiltani.

Az önkormányzati ASP szakrendszereihez történő csatlakozás többtényezős hitelesítéssel történik. A felhasználónak rendelkeznie kell E-személyi-vel, valamint kártyaolvasóval.
Az E-személyihez csak a hozzá tartozó PIN kód megadásával lehet hozzáférni. A PIN kód megadása után. A sikeres azonosítást és hitelesítést követően az ASP rendszer az egyes szakrendszerekhez történő hozzáférés során további azonosító adatokat (felhasználói név, jelszó) kérhet.

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

A Hivatal jelszókezelő rendszere:
a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;
b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;
c) kényszerítse ki a megfelelő minőségű jelszavak használatát;
d) kényszerítse ki a jelszóváltoztatást;
e) tiltsa meg a korábban használt jelszavak ismételt felhasználását;
f) beíráskor ne jelenítse meg a jelszavakat a képernyőn;
g) a jelszó állományokat rejtjelezve tárolja;
h) változtassa meg a szállító alapértelmezett jelszavát a szoftver installálása után.
Jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni, úgy, hogy:
a) szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;
b) biztosítani, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:
a) a jelszó legalább nyolc karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;
b) a jelszavakat 60 naponta meg kell változtatni;
c) a jelszavakat két napon belül nem szabad megváltoztatni;

d) az előző jelszavak újra használatát kerülni kell;
e) zárolás esetén előre beállított időtartam eltelte után engedélyezze vissza a felhasználói fiókot.

5. A felhasználó felelőssége a jelszó használat során

A Hivatal elektronikus információs rendszereiben a jelszavak használatának és képzésének részletes szabályai a következők:
a) a felhasználó a jelszavát köteles titokban tartani;
b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben;
c) a felhasználói jelszót TILOS leírni;
d) ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni és értesíteni kell az IBF-et;
e) nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;
f) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el. Ennek érdekében az alábbi szempontokat kell betartani:
g) könnyen megjegyezhető, és nehezen kitalálható legyen;
h) semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;
i) ne legyen a gépnévre vagy a felhasználói névre utaló;
j) ne legyen sorozat.
Különös figyelmet kell fordítani az E-személyihez tartozó PIN kód titokban tartására, mivel az E-személyivel minősített elektronikus aláírás hozható létre, mely teljes bizonyító erejű magánokiratnak megfelelő joghatással bír.

A fenti szabályok az elektronikus információs rendszerek által technikailag kikényszeríthető részét az információbiztonsági felelősnek kell biztosítani.
A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben.

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat az információbiztonsági felelős hozza létre. Az azonosítók ismételt felhasználása tilos. 2 hónap inaktivitás után az azonosítókat le kell tiltani.

Az illetéktelen hozzáférések elkerülése érdekében olyan hitelesítési módszereket kell alkalmazni, amely a sikertelen bejelentkezési kísérletekről nem ad vissza semmilyen olyan érdemi információt, amelyet egy támadó ki tud használni és illetéktelenül hozzá tud férni a Hivatal elektronikus információs rendszereihez.
Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie az érintett szervezeten kívüli felhasználókat, illetve a tevékenységüket.

6. Hitelesítés szolgáltatók

A Hivatal elektronikus információs rendszereihez az Internet irányából csak szabványos, kriptográfiai módszerrel azonosított és hitelesített felhasználó, titkosított hálózati kapcsolaton keresztül lehet hozzáférni. A nem a hivatal állományában lévő felhasználó külső hozzáférése esetén a hálózati kommunikáció titkosításához csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

7. Hozzáférés ellenőrzés

A hozzáférési jogok kezelését jelen eljárásrendben foglaltak szerint kell megvalósítani a következő alapelvek alkalmazásával:
a) Minden felhasználó csak a feladatellátásához szükséges, minimális jogosultságot kapja meg.
b) A felhasználók a munkaállomásukon nem rendelkezhetnek rendszergazda jogokkal.
c) A rendszergazda a rendszerek adminisztrálásához használt adminisztrátori azonosítóját a napi munkavégzése során nem használhatja. A napi munkavégzéshez normál felhasználói jogú azonosítót kell használnia.
d) Az önkormányzati ASP szakrendszerekhez történő hozzáféréseket a működtető által megfogalmazott eljárásrend alapján kell kezelni.

8. Felhasználói fiók kezelése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.
A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:
a) A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.
b) Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.
c) Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.
d) Az összeférhetetlenségi szabályokat figyelembe kell venni.
e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.
f) Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén, papír alapon kell a nyilvántartást vezetni.
g) Minden egyes elektronikus információs rendszerhez, csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.
h) Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

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

A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.
A csoportos felhasználó azonosítók használatát tiltani kell.
A felhasználói hozzáférési jogosultságokat a jegyző határozza meg.

A jogosultság meghatározása során figyelembe kell venni:

- a felhasználó munkakörét és az azzal kapcsolatos feladatait;
- a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;
- a felhasználó jogviszonyát;

A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell:

- a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;
- annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;
- azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör, vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;
- annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;
- a munkahelyi vezető aláírását.

A jogosultságigénylési lapot az igényelt és a beállított jogosultságok egyeztetése céljából az információbiztonsági felelős tárolja.

9. Kiemelt jogosultságok kezelése

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

Az elektronikus információs rendszereknél a jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:
a) pontosan meg kell határozni azokat a rendszerelemeket, - pl. operációs rendszereket, adatbázis kezelő rendszert, valamint az alkalmazásokat - és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni;
b) az adminisztrátori jogosultságokat a „feltétlenül szükséges" és az „eseményenkénti" használat elve alapján kell kiadni;
c) az adminisztrátori jogot kizárólag a jegyző engedélyezheti írásban.
Az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá, a részükre biztosított adminisztrátori jogosultság birtokában csak a felhasználó külön engedélyével és jelenlétében, kifejezetten a hiba elhárítása érdekében vagy a felhasználói igény kielégítése érdekében férhetnek hozzá a felhasználók által kezelt információkhoz.
A rendszergazda nem küldhet levelet más felhasználó nevében.

10. ASP rendszerek hozzáférése

Az ASP szakrendszerekhez történő hozzáférés feltétele, hogy a felhasználó rendelkezzen E-személyivel, melyet az okmányirodákban és a kormányablakokban igényelhet.
ASP szakrendszerekhez történő hozzáférések esetében az új felhasználó létrehozását az önkormányzati ASP adminisztrátornak kell jelezni az igényelt szakrendszer és a szakrendszeri szerepkör megadásával, aki a szükséges hozzáférés birtokában létrehozza a felhasználót az ASP rendszerben, illetve hozzárendeli a szakrendszeri szerepkörökhöz.
Beállítandó jogosultsági elemek:

a) Szakrendszerekhez való hozzáférés:
Mely szakrendszerekhez vagy keretrendszeri modulokhoz férhet hozzá a felhasználó.

b) Szerepkörök szakrendszerenként:
Összehangolt szerepkör-megnevezések (cél a jó áttekinthetőség)
Ugyanannak a felhasználónak több szerepköre is lehet

c) Iktatóhelyekhez (iktatási sávokhoz) való hozzáférés:
A felhasználó csak a megadott iktatóhelyek iratainak kísérőadatait tekintheti meg.

d) Szervezeti egységekre vonatkozó vezetői jogosultságok:
Az iratokba való betekintési jog az előadón kívül az előadó mindenkori vezetőjét is megilleti

e) Helyettesítési jogosultságok:
Szabadságolások kezelése, munkahelyi vezető és titkárnő kapcsolata, közeli munkatársak feladatmegosztása.
A módosító műveletek automatikus naplózásakor a helyettesítő kiléte is tárolódik.

Az ASP szakrendszerek esetében az önkormányzati ASP adminisztrátor nyilvántartást vezet jogosultságokról.

A nyilvántartás a következő elemeket tartalmazza:

a) szakrendszer megnevezése;
b) felhasználó neve, beosztása;
c) szerepkör megnevezése (esetleg többlet jogosultságok);
d) jogosultság beállításának dátuma.

A kilépő felhasználókról a személyügyi ügyintézőnek értesítenie kell az önkormányzati ASP adminisztrátort, aki visszavonja a kilépő felhasználó jogosultságait.
A kiosztott jogosultságokat az önkormányzati ASP adminisztrátor évente felülvizsgálja és - az adatgazdákkal egyeztetve - a nem szükséges jogosultságokat visszavonja.

10.1. Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését űrlap kitöltésével kezdeményezi. Hozzáférési jogot az igényelhet, akinek a feladatellátásához az szükséges.

Az űrlapon meg kell jelölni az igényelt jogosultság szintjét, azt az időszakot, amelyre a jogosultságot biztosítani kell, illetve a jogosultságigénylés indoklását.
A kitöltött űrlapot alá kell írattatni a munkahelyi vezetővel, aki igazolja, hogy a feladatellátáshoz szükséges a jogosultság biztosítása.
Az űrlapot ezután meg kell küldeni az adatgazda részére, aki jóváhagyja a jogosultságigénylést.
A jóváhagyott jogosultságigénylési űrlapot ezután el kell küldeni rendszergazda részére, aki intézkedik a jogosultság kiadásáról.
A rendszergazda az igényelt beállításokkal létrehozott felhasználói fiókról telefonon vagy személyesen értesíti az igénylőt, és megadja a belépéshez használatos felhasználói nevet, és az első belépést lehetővé tevő kezdeti jelszót és szükség esetén egyéb fontos adatokat.
Az aláírt űrlapok ezek után az információbiztonsági felelősnél kerülnek tárolásra visszakereshető formában.
Az IBF az említett adatlapok meglétét és a tényleges jogosultság kiadását bármikor ellenőrizheti, és véleményét írásba foglalhatja, amelyet az Hivatal a jogosultsági rendjének folyamatos javítására használ fel.

10.2. Hozzáférési jog módosítása, visszavonása

A munkahelyi vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a *Jogosultságigénylési űrlap}* mellékletét. Az eljárásrend megegyezik az *Új hozzáférési jog igénylése}* fejezetben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

A hozzáférési jog visszavonásra kerül a feladatkör megváltozása, munkaviszony megszűnése, két hónapnál hosszabb tartós távollét (Gyes, GYED) esetén.

11. Azonosítás vagy hitelesítés nélküli tevékenységek

A Hivatalban nem engedélyezünk azonosítás és hitelesítés nélküli tevékenységet.

12. Külső elektronikus információs rendszerek használata

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

a) Az eszközökön a felhasználóknak rendszergazdai jog nem adható.
b) Az eszközökön naprakész kártékony kód elleni védelmet kell megvalósítani.
c) Az eszközökön az operációs rendszer és a felhasználói programok naprakészségét biztosítani kell.
d) Az eszközökön bekapcsolt tűzfalat kell alkalmazni.

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

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

13. Naplózási eljárásrend

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

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

a) a felhasználók adminisztrációs tevékenysége:
- bejelentkezés;
- kijelentkezés;
- jelszómódosítás.

b) az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;
c) a rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;
d) a rendszergazdák tevékenysége a rendszer bármely rétegében;
e) a felhasználói jogosultságok módosítása;
f) rendszer események, esetleges hibák;
g) konfigurációs beállítások módosítása.
h) Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóba kell rögzíteni.
Az elektronikus információs rendszerek naplózása kialakításakor be kell vonni a rendszer adatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyeket az adatgazdák igényelnek.

13.1. Naplóbejegyzések tartalma

A naplóbejegyzéseknek a következőket kell tartalmaznia:
a) a rendszerelem azonosítóját,
b) az adatazonosítót (fájl / rekord / mező),
c) az esemény ismertetését / a funkcióazonosítót,
d) a felhasználó azonosítóját,
e) az esemény időpontját,
f) az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

Az elektronikus információs rendszereknek a naplóbejegyzésekhez készített időbélyegeket a rendszer belső órái alapján kell elkészítenie.
A Hivatalnak szinkronizálnia kell a rendszer belső rendszer órákat a belső, illetve a külső időszolgáltatóval.

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

Olyan elektronikus információs rendszereket kell alkalmazni, melyek
a) biztosítják a naplóbejegyzések előállítási lehetőségét
meghatározott naplózható eseményekre;
b) lehetővé teszik meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;
c) naplóbejegyzéseket állít elő meghatározott tartalommal.

14. Rendszer és információ sértetlenségére vonatkozó eljárásrend

A rendszerprogramokkal kapcsolatos bármely konfigurálási, hangolási műveletet csak a rendszergazda végezhet. Az alkalmazáson végzendő, annak bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is - a jegyző engedélye szükséges.
A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára.
Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.
A felhasználói adatok és alkalmazások védelme érdekében a szoftverek módosítása (frissítés, verzióváltás) folyamán az alkalmazáshoz és az adatokhoz történő illetéktelen hozzáférést és az illetéktelen próbálkozást meg kell akadályozni. Gondoskodni kell arról, hogy a telepített alkalmazások, fájlok ne károsodjanak, és a követelményeknek megfelelően működjenek.
Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.
Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

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

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

IV.
VÍRUSVÉDELMI ELJÁRÁSOK

1. Kártékony kódok elleni védelem

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

A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:
a) Munkaállomások és kiszolgálók esetében memóriában rezidens kártékony kód elleni megoldásokat kell alkalmazni.

b) Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.
c) Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.
d) A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.
e) A kártékony kód elleni alkalmazásnak az e-mail-ek csatolmányát ellenőriznie kell, a futtatható állományok szűrését be kell kapcsolni.
f) A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.
g) A külső forrásból származó a cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.
h) A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.
i) A kártékony kód felfedezésekor az információbiztonsági felelőst értesíteni kell.
j) Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani a hivatali hálózatról és így kell megtenni a szükséges vírusirtást vagy a rendszer újratelepítését.
k) A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

2. Szervezetünknél a használt vírusvédelmi szoftverek

A szoftver teljes számítástechnikai gépparkot lefedő (beleértve a mobil eszközöket is) telepítéséért, naprakész és folyamatos üzemeltetéséért, frissítéséért, a vírustámadások elleni védekezés megszervezéséért a rendszergazda felelős. Az újonnan vásárolt számítógépekre azok rendszerbe állítása során telepíteni kell a víruskereső programot.

A számítógépes munkaállomásokon a víruskereső programot úgy kell beállítani, hogy naponta egyszer (az első bejelentkezéskor) megtörténjen az automatikus vírusteszt futtatása. A rendszerbe kívülről bekerülő adatokat (USB portról csatlakoztatható eszközök, CD-ROM, Internet stb.) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső program munkaállomásokon történő lefuttatása a felhasználó feladata és felelőssége.
A víruskereső szoftvernek minden lehetséges bejutási pontot (USB portról csatlakoztatható eszközök, CD-ROM, hálózat, e-mail, stb.) ellenőriznie kell, így az elsődleges támadási felületnek minősülő munkaállomásokat, és a másodlagos támadási felületnek minősülő tűzfalakat, alkalmazás és levelező szervereket.
A vírusadatbázisok frissítése a rendszer hatékony működésének szempontjából fontos, mivel az új vírusok megjelenése és elterjedése között rövid idő (esetenként néhány óra) telik el.

3. A vírusvédelem szabályai a felhasználó részéről

Biztosítani kell, hogy a szervezetnél alkalmazott vírusvédelmi rendszer a számítógépek működése közben folyamatosan dolgozzon, így a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül már a használat előtt vírusellenőrzése kerülnek. A számítástechnikai eszközökön beállított aktív védelemi rendszer kikapcsolása tilos. A rendszer kikapcsolásából adódó károkért (adatvesztés, illetéktelen hozzáférés stb.) a szabályt megszegő teljes körű felelősséggel tartozik.

Amennyiben a felhasználó a víruskereső program *„futtatása"* során vírust észlel, azonnal jelentenie kell az informatikai munkatárs felé, aki feljegyezi a vírus és a fertőzött file nevét, továbbá a munkaállomás számát (helyét). Az informatikai munkatárs gondoskodik a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

4. Az elektronikus levelezés vírusvédelme

Ha a szervezet elektronikus levelezési rendszerén keresztül fertőzött levél, vagy csatolt állomány érkezik, arról a víruskereső szoftver értesíti a felhasználót. Ha az aktív védelem a fertőzött állományt eltávolítja, akkor a munka megkezdhető vagy tovább folytatható, amennyiben nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt törli.
Ha a felhasználó levelezési rendszerébe indokolatlan vagy váratlan e-mail érkezik annak tartalmát személyesen (pl. telefonon, e-mailben) ellenőrizni szükséges. Ha a küldő nem szándékosan mellékelt az e-mailhez állományt, akkor nem szabad megnyitni.

5. Vírusriadó

Abban az esetben, ha egyértelműen megállapítható, hogy a tapasztalt jelenségeket vírusfertőzés okozza, de a vírus egy-két gépet fertőzött csak meg, akkor vírusriadót nem szükséges elrendelni.
A fertőzött gépeket azonnal le kell kapcsolni a hálózatról, meg kell kísérelni a vírusok kiirtását.
Ha ez nem sikerül, akkor vírusriadót kell elrendelni.
Feltétlenül vírusriadót kell elrendelni a következő esetek bármelyikénél:
a) ha a szokásosnál sokkal több vírusincidens történt;
b) a vírusfertőzést magas kockázatúnak értékeli a vírusvédelmi szoftver gyártója
c) ugyanaz a vírus fordul elő egyszerre kettőnél több gépen, különböző állományokban;
d) valamely számítógépen aktivizálódik a vírus romboló rutinja, vagy a vírus valamilyen effektust (videó, hang stb.) produkál annak ellenére, hogy a vírusadatbázis frissített, a víruskereső motor működött;
e) adatátvitel során, egy számítógépen jelentkező szokványostól eltérő működés, átkerül más számítógépekre is;
f) szerver oldali vírusfertőzés esetén.
A vírusriadó idején a vírus mentesítés szakmai felügyeletét az IBF és a rendszergazda közösen látják el.

Az IBF feladata a vírus fertőzés kivizsgálásának irányítása, a felelősség megállapítása.
A rendszergazda a feladatai:
a) a vírusvédelmi rendszer támogatójának értesítése;
b) a vírus fertőzés következtében szükséges intézkedések koordinálása;
c) a fertőzés tényének és a foganatosított intézkedéseknek a rögzítése;
d) a vírusos számítógép leválasztása a hálózatról;
e) a felhasználók értesítése a vírusról;
f) az e-mail rendszer leállítása, ha mail-ben terjedő vírusról van szó;

g) a hálózaton terjedő vírus esetén a külső kapcsolat megszakítása;
h) a vírus adatait tartalmazó vírus tudásbázis letöltése és teljes vírusellenőrzés végrehajtása;
i) a fertőzöttség lehetőségeinek feltérképezése, gondolva a hálózaton, cserélhető adathordozók által, vagy e-mail-en történő fertőzésekre;
j) a kliensek frissítése;
k) manuális vírus ellenőrzés végrehajtása azokon a munkaállomásokon, amelyek megfertőződhettek;
l) amennyiben az a hivatalon kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;
m) a vírus fertőzés okának kivizsgálása a vírusvédelmi szoftver támogatójával közösen.

V.
RENDSZER ÉS KOMMUNIKÁCIÓ VÉDELEM

1. Internet Etikai Kódex

Minden Internet szolgáltatás előfizetőjének, igénybevevőjének az Internet nemzetközi számítógépes hálózat használata során be kell tartania a hálózati viselkedés általános etikai szabályait. Az Internet hálózat olyan módon történő használata, amely sérti ezeket a szabályokat, az információkat szolgáltató-szervereken nyomon követhető, és a szabályok be nem tartása az igénybevevő Internet szolgáltatójának figyelmeztetését, illetve az Internetből való kizárását, a szerződés egyoldalú – és azonnali – felmondását vonhatja maga után.

2. Internet használata

A szervezeténél a munkatársak a saját gépeiken internet hozzáféréssel rendelkeznek. A bejelentkezés egyedi felhasználói azonosítóval, és jelszóval történik.

Az Internet használatának kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni az Internetet. A Weben található tartalom egy része potenciális veszélyforrás. A veszélyes oldalak körét nem lehet behatárolni, de a felhasználó köteles távol tartani magát a szerencsejátékot tartalmazó oldalaktól, valamint a közösségi, videomegosztó, és blog oldalaktól stb.
A belső hálózat irányából az internet irányába kapcsolatot csak azokra a protokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.
Kifejezetten tilos a belső hálózat irányából az internet irányába a levelezési (SMTP) kapcsolat. Levelet továbbítani csak a levelező szerveren keresztül szabad. Megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;
A felhasználókat jelszóval megfelelően hitelesíteni kell;
Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.
A Hivatal belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.
Biztosítani kell, hogy a Hivatal elektronikus információs rendszerei alapértelmezés szerint ne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükséges igény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.
Minden Internet elérést naplózni kell, annak érdekében, hogy kellő mennyiségű információt

lehessen összegyűjteni a szabálytalan internetes tevékenységek detektálása és kiderítése érdekében.
Kiemelt figyelmet kell fordítani a tűzfal operációs rendszere biztonsági frissítéseinek figyelésére és telepítésére.
A tűzfalat úgy kell konfigurálni, hogy az utasítsa el a port letapogatási próbálkozásokat.
A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

A felhasználónak az Internet használata során tilos:

A Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele,

- Az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni,
- Fájlcserélő alkalmazásokat futtatni, illetve nem hivatali munkavégzéshez szükséges letöltéseket végezni,
- Hivatali email címmel nyilvános levelezőlistákra, hírlevelekre feliratkozni.
- A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.
- Az IBF köteles ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.
- A Hivatal központi tűzfalát csak a belső hálózatból vagy a konzolról lehet adminisztrálni. A külső hozzáférés nem engedélyezett.

3. E-mail használata

Az e-mail használatának kizárólagos célja a munkavégzés. A felhasználó nem jogosult magáncélra használni a levelező rendszert. A szervezetnél kiosztott minden email cím a munkavégzést a szervezet ügyinek intézését szolgálja függetlenül attól, hogy egy-egy felhasználó személyéhez kötött az elnevezés. A munkáltató jogosult a email címmel és az ottani adatokkal minden egyéb műveletre is. A felhasználó munkavállaló nem jogosult a szervezet levelezését kívülre átirányítani.

A felhasználó nem jogosult a szervezet belső informatikai rendszerén kívüli helyszínen, vagy helyszínről publikus eszközről, vagy publikus csatornán elérni leveleit, sem egyéb belső informatikai szolgáltatást, kizárólag a szervezet igényei szerint megfelelően védett eszközről, védett csatornán.

Biztonságos eszköz a saját otthoni, vagy mobil számítógép amennyiben a belső eszközökkel azonos védelmi eszközökkel rendelkezik, és nincs másik felhasználója. Nem biztonságos eszköz internet terminál, más cég, szervezet számítógépe.

A felhasználó nem jogosult a szervezeten kívüli levelezését elérni, csak úgy hogy a szervezet mail címére átirányítja a külső leveleket.

4. Mobil eszközök használata

A mobil eszközök abból adódóan, hogy használatba kerülhetnek a belső védett környezeten kívül is, különös körültekintést igényelnek. A mobil eszközöket a Hivatalban csak írásos jegyzői engedéllyel lehet használni. A szervezet területén kívül a felhasználó felelős a mobil eszköz fizikai védelméért, lopás elleni védelméért, és a megfelelő környezetben való használatért. A mobil eszközt autóban hagyni, nyilvános helyen lopás lehetőségének kitenni tilos. A mobil eszközt tilos úgy idegen hálózaton használni, hogy a felhasználó nem bizonyosodott meg az előírt adatvédelmi eszközök helyes működéséről a mobil eszközön.
A mobil eszköz elvesztését a jegyzőnek írásban jelenteni szükséges.
A Hivatal belső hálózatához idegen (nem a hivatal tulajdonában lévő) infokommunikációs eszköz nem csatlakoztatható.

5. ASP hálózati eszközök használata

Az ASP rendszer eléréséhez szükséges eszközöket (ASP router, switch, szünetmentes tápegység) zárt rack szekrényben kell működtetni.
A rack szekrények kulcsait az információbiztonsági felelős őrzi.

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

- az eszközök hálózatba illesztéséről készüljön dokumentáció;
- az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek
- megváltoztatásra;
- a hozzáférési azonosítókat zárt borítékban, és biztonságosan zárható helyen kell tárolni;
- a hálózati eszközöket csak az információbiztonsági felelős, valamint szerződésben a hálózati eszközök karbantartására kijelölt fél(rendszergazda) kezelheti;
- az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történjen meg;
- a menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva;
- az ASP rendszerhez csatlakozó munkaállomásokat menedzselhető hálózati eszközökre kell kötni;
- ezeken az eszközökön - az idegen eszközök hálózatba történő csatlakozása elleni védelem megvalósítása érdekében - be kell kapcsolni a port security megoldást.

5. 1. Hálózat szegmentálás

A Hivatal hálózatában az infokommunikációs szolgáltatásokat, felhasználókat és elektronikus információs rendszereket szegmentálni kell. A külső felhasználók Internet irányából csak a szükséges elektronikus információs rendszereket érhetik el. A belső hálózatot tűzfal válassza el a többi zónától. Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom szűrésére, a lehetőségek korlátozására tűzfalak, tartalomszűrők, illetve meghatározott címekkel a kapcsolat tiltását biztosító megoldások szolgálnak.

6. E-személyi kezelése

Az önkormányzati ASP rendszerhez történő csatlakozás során használandó E-személyi kezelését a következő szolgáltatói dokumentumok szabályozzák:

- Általános szerződési feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI) v1.6
- Szolgáltatási szabályzat a személyazonosító igazolványokhoz kibocsátott minősített
- tanúsítványokhoz (HSZSZ-ESZIG) v1.3
- Hitelesítési rend a személyazonosító igazolványokhoz kibocsátott minősített
- tanúsítványokhoz (HR-ESZIG) v1.3
- Időbélyegzés Szolgáltatási Rend (ISZR) v1.2
- Szolgáltatási szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz
- (HSZSZ-M) v1.6

7. Mobilkódok alkalmazása

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

- Java Applet
- JavaScript
- VB Script
- CGI
- ActiveX
- Shockwave
- Flash

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

- Előreugró ablakok - blokkolás
- Mikrofonok, kamerák hozzáférése - tiltás
- Automatikus letöltés - rákérdezés

A web böngészők fentieknek megfelelő biztonsági beállítása az információbiztonsági felelős ill. a megbízott rendszergazda a felelős.
A web böngészők helyes beállításait az IBF-nek ellenőriznie kell.

VI.
ZÁRÓ RENDELKEZÉSEK

Ez a szabályzat 2019. január 1-én lép hatályba.

A szervezetnél a jegyző köteles gondoskodni arról, hogy e szabályzatot valamennyi munkatárs és az informatikai feladatokat ellátó szerződött partner megismerje, és ennek tényét a szabályzathoz csatolt íven aláírásával igazolja a hatálybalépés napját megelőzően.

Szilsárkány, 2018. december 20.

Szilsárkányi Közös Önkormányzati Hivatal * Szilsárkány *

dr. Horváth Martina
jegyző

MELLÉKLETEK

1. sz. melléklet- Szoftver nyilvántartás
2. sz. melléklet – Titoktartási Nyilatkozat
3. sz. melléklet – Biztonsági események jelentése
4. sz. melléklet – Jogosultságigénylési űrlap
5. sz. melléklet – Hozzáférések nyilvántartása űrlap
6. sz. melléklet – Felhasználói Nyilatkozat
7. sz. melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén
8. sz. melléklet – Kockázatok és intézkedések nyilvántartása

1. sz. melléklet

Szoftver Nyilvántartási Adatlap

A szoftvernyilvántartási adatlap a válallkozás által használt szoftverek licenceit tartalmazza, és egyben igazolja, hogy a vállalkozás az alább felsorolt szoftver licencek jogos felhasználója. A szoftver nyilvántartási adatlap felhasználható egy esetleges hatósági ellenőrzésnél a szoftver licencek eredetének igazolására, illetetve a vállalkozás könyvelésében szereplő immateriális javak nyilvántartásának mellékleteként.

A SZERVEZET ADATAI

SZERVEZET NEVE:

CÍM :

CÍM :

A NYILVÁNTARTÁST VÉGZŐ NEVE:

A NYILVÁNTARTÁST VÉGZŐ E-MAIL CÍME:

FELHASZNÁLÓ ADATAI

FELHASZNÁLÓ NEVE:

SZÁMÍTÓGÉP AZONOSÍTÓ

FELHASZNÁLÓI PROFIL

FELHASZNÁLÓ E-MAIL CÍME:

SZOFTVER GYÁRTÓJA	SZOFTVER NEVE ÉS VERZIÓSZÁMA	A SOFTVER SOROZATSZÁMA, AZONOSÍTÓJA	NYELV	TELJES LICENC VAGY FRISSÍTÉS	LIICENCEK SZÁMA	LICENC KONSTRUKCIÓ	EREDETISÉGET IGAZOLÓ OKIRAT (SZÁMLASZÁM, SZERZŐDÉSSZÁM)	TELEPÍTÉS/UPGRADE DÁTUMA	TELEPÍTŐ/FRISSÍTŐ SZERVEZET

Kijelentem, hogy a jelen űrlapon általam megadott adatok helyesek, és a valóságnak megfelelően tükrözik a Szervezet szoftverállományának állapotát

JOGSZABÁLYOK

A jogszabályok elérhetősége a következő:

- 2013. évi L. törvény
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV
- 41/2015. (VII. 15.) BM rendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500041.BM
- 257/2016. (VIII. 31.) Korm. rendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600257.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

2. számú melléklet

TITOKTARTÁSI NYILATKOZAT
Külső szerződő partner részére

Alulírott
Név:.....
Anyja neve:.....
Lakcím:.....
Sz. ig. szám:.....
a ..... munkatársa kijelentem, hogy a **Szilsárkányi Közös Önkormányzati Hivatal,** mint **Megrendelő,** valamint .....mint **Vállalkozó** között.....tárgyú, ... **-én megkötött vállalkozási/megbízási/szállítási szerződés** keretében elvégzett feladatok során tudomásomra jutott információkat és adatokat bizalmasan kezelem és megtartom. A tudomásomra jutott információkat, adatokat az érdekkörön kívüli személlyel nem közlöm. Ezen felelősségem fennáll azt követően is, ha a ..... -vel való szerződéses jogviszonyom bármely okból megszűnik.

Szilsárkány, 201 .....

.....
Nyilatkozó

Tanú 1
Aláírás:
Név:
Szem.ig.szám:
Lakcím:

Tanú 2

3. sz melléklet

A biztonsági esemény jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és idő pontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:

Észlelő aláírása IBF aláírása

Az esemény kivizsgálásának leírása:

Megtett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:
Igen
Nem

Igényel-e kockázatelemzést az esemény:
Igen
Nem

Dátum:

Információbiztonsági felelős aláírása jegyző aláírása

4. sz melléklet

Hozzáférési jogok igénylése űrlap

Iktatószám:
Jogosultságigénylő adatai
Igénylő neve: .....
Szervezeti egység: .....
Telefon: .....
E-mail: .....
Igényelt művelet
Jogosultság kezdete: ..... Jogosultság vége:.....
Új jogosultság
Jogosultság törlése
Jogosultság módosítása
Egyéb:.....
.....
.....
Indoklás
A jogosultságigényléshez kapcsolódó feladatellátás megnevezése:
.....
.....
.....
Kelt: ..... igénylő aláírása

Adatgazdai jóváhagyás
Adatgazda: ....
Kelt ..... adatgazda aláírása
A jogosultságot beállító aláírása
Rendszergazda/IBF: ....
Kelt ..... rendszergazda/IBF aláírása

5. sz. melléklet

HOZZÁFÉRÉSEK NYILVÁNTARTÁSA

Sorszám	Felhasználó neve	Igényelt jogosultság	Jogosultság kezdete	Jogosultság megszüntetése	Megjegyzés

6.sz. melléklet

Információbiztonsági tájékoztató jogviszony megszűnése esetén

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

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

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

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

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

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

Szilsárkány, 201 ... . jegyző

A fenti tájékoztatást tudomásul vettem:

Szilsárkány, 201 ... . köztisztviselő

7. sz. melléklet

A KOCKÁZATOK ÉS INTÉZKEDÉSEK NYILVÁNTARTÁSA

Sorszám	Kockázatok	Bekövetkezés valószínűsége	Felmerülő kár mértéke	Kockázat kezelésére javasolt intézkedés	Határidő	Felelős munkatárs neve

Megismerési nyilatkozat

Az Informatikai Biztonsági Szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás
DR. HORVÁTH MARTINA	FEGYZŐ	2019.01.02.	dr. Horváth Martina
SZŐDELYI GABRIELLA	VEZETŐ FŐ TANÁCSOS	2019.01.02.	Sződelyi Gabriella
RONCS TIBORNÉ	GAZD. FŐ EA.	2019.01.02.	Roncs Tiborné
PAPAI DÓRA	GAZD. EA.	2019.01.02.	Papai Dóra
LUKA MARTINA	IG. EA.	2019.01.02.	
NYÍRI KLAUDIA	GAZD. EA.	2019.01.02.	Nyíri Klaudia
SZALAI MIKLÓS	POLGÁR-SZOLG. MESTER	2019.01.02.	
VARGA IMRE ROBERT	POLGÁRMESTER BOGYOSZLÓ	2019.01.02.	
DÓCZY GÉZA	POLGÁRMESTER DÖRÖ	2019.01.02.	Dóczy Géza
HOLNÁK VILMOS SÁNDOR	POLGÁRMESTER POTTOND	2019.01.02.	Holnák Vilmos Sándor
DUDÁS KINGA	IG. EA.	2019.08.09.	Dudás Kinga
DR. BALCZNÉ VARGA-DUDÁS KATALIN	IG. EA.	2022.02.01.	Dr. Balczné Varga-Dudás Katalin
