

HITELESÍTÉSI ZÁRADÉK

Az eredeti papíralapú dokumentummal egyező hiteles másolat.

Iktatószám: 04/3495-3/2022

Másolatkészítő szervezet: Bonyhádi Közös Önkormányzati Hivatal

Másolat hitelesítését végző személy: Dr. Márton Antal - marton.antal@bonyhad

Másolatkészítés időpontja: 2022.12.07. 15:54

Másolatkészítő rendszer megnevezése: ASP IRAT Szakrendszer

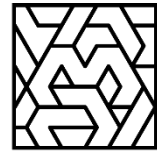
Másolatkészítő rendszer verziószáma: 21.2.0.32

Másolatkészítési szabályzat megnevezése: Bonyhádi Közös Önkormányzati Hivatal Jegyzőjének 6/2020. (III.1.) utasítá...

Másolatkészítési szabályzat verziószáma: 1

Másolatkészítési rend elérhetősége: <http://www.bonyhad.hu/dokumentumtar/szabalyzatok.html>

Bonyhád Város Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasítása
Bonyhádi Közös Önkormányzati Hivatal és
Bonyhád Város Önkormányzata
Informatikai Biztonsági Szabályzatáról



MAXENTROP KFT



BONYHÁDI KÖZÖS ÖNKORMÁNYZATI HIVATAL ÉS BONYHÁD VÁROS ÖNKORMÁNYZATA INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Iktatási szám: 15/275-3/2021

Dátum: 2021.10.01

Készítette: Maxentrop Kft.

Tartalomjegyzék

1.	Az Informatikai Biztonsági Szabályzat	3
1.1.	A dokumentum célja.....	3
1.2.	A dokumentum hatálya	4
1.3	A dokumentum minősítése, kötelezettségek.....	5
1.4	Alapfogalmak.....	5
1.5	Kapcsolódó dokumentumok	8
1.6	Szerepkörök.....	10
1.7	Tevékenységek	14
1.8	Hivatalrendszer belső együttműködése.....	14
2	Hivatal besorolási Nyilatkozata.....	15
3	Rendszerek besorolási nyilatkozata.....	16
4	Adminisztratív Védelmi Intézkedések.....	18
4.4	Szervezeti szintű alapfeladatok	18
4.5	Informatikai biztonsági szabályzat	18
4.6	Az elektronikus információs rendszerek biztonságáért felelős személy	18
4.7	Intézkedési terv és mérföldkövei.....	18
4.8	Az elektronikus információs rendszerek nyilvántartása	18
4.6	Rendszer és szolgáltatás beszerzés.....	19
4.7	Üzletmenet- (ügymenet-) folytonosság tervezése	20
4.8	Az elektronikus információs rendszer mentései	22
4.9	Emberi tényezőket figyelembe vevő – személy – biztonság.....	25
4.10	Tudatosság és képzés.....	29
5	Fizikai Védelmi Intézkedések.....	30
5.1	Fizikai és környezeti védelem	30
6	Logikai Védelmi Intézkedések	36
6.1	Tervezés.....	37
6.3	Konfigurációkezelés	40
6.5	Karbantartás	43
6.6	Azonosítás és hitelesítés.....	47
6.7	Hozzáférés ellenőrzése.....	48
6.8	Rendszer- és információsértetlenség.....	51
6.9	Naplózás és elszámoltathatóság.....	53
6.10	Rendszer- és kommunikációvédelem	55

1. Az Informatikai Biztonsági Szabályzat

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

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

Területi hatálya:

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata
Tolna megye 7150 Bonyhád, Széchenyi tér 12.

1.1. A dokumentum célja

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

A Szabályzat további célja, hogy iránymutatással szolgáljon a Hivatal informatikai rendszereihez hozzáférési jogosultsággal rendelkező felhasználók számára az informatikai rendszerek helyes használatáról, ismertesse a helyes és biztonságos munkavégzés szabályait, a követendő eljárásokat, továbbá rögzítse a felhasználókkal szemben támasztott elvárásokat és követelményeket. Meghatározza a Hivatal részére az elektronikus információbiztonsággal kapcsolatos elveket, szabályokat, au elvárt és betartandó magatartásformákat és gyakorlatokat.

A Bonyhádi Közös Önkormányzati Hivatalban (a továbbiakban: Hivatal) üzemelő számítástechnikai infrastruktúra hátteret teremt a Hivatalban folyó munkavégzéshez, de mindez csak az informatikai eszközök biztonságos, szabályozott működése mellett válik valóságos előnnyé.

Az információk, illetve adatok rendelkezésre állását, elérhetőségét az arra jogosult felhasználók számára különösen az alábbi feltételek biztosításával kell lehetővé tenni:

- a feladat ellátásához szükséges és elégséges jogkörök,
- az információk, illetve adatok sértetlensége (sérthetetlensége, valódisága),
- az információknak, illetve adatoknak jellegüktől függő bizalmas kezelése,
- az információk és adatok hitelessége, valamint a teljes informatikai, illetve információs rendszer működőképessége.

Készítette: Maxentrop Kft.

A szabályzat célja továbbá, hogy az informatika alkalmazása során biztosítsa a Hivatalban az alábbiakat:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- munkaállomásokon lekérdezhető adatok körének meghatározását,
- adatállományok biztonsági mentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

1.2.A dokumentum hatálya

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

- a védelmet élvező elektronikus adatok teljes körére, felmerülési és feldolgozási helyüktől, idejüktől és fizikai megjelenési formájuktól függetlenül,
- a Hivatal tulajdonában, vagy más módon használatában lévő eszközre,
- a fenti eszközök, műszaki dokumentációira,
- az információs rendszerek fejlesztési, szervezési, programozási, üzemeltetési dokumentációira,
- a rendszer és felhasználói programokra,
- és min ezek védelmét szolgáló (beleértve e dokumentumot is) gyakorlati ismeretekre és vagy ezek dokumentációira.

A Szabályzat **személyi hatálya** kiterjed valamennyi, a feladatai ellátásához a Hivatal informatikai rendszereit, eszközeit használó, vagy azokhoz hozzáférő köztisztviselőkre, Munka Törvénykönyve hatálya alá tartozó munkavállalóra, továbbá a Hivatalban megbízási, vagy egyéb jogviszony vagy vállalkozói szerződés alapján az informatikai rendszerekhez bármilyen okból hozzáférő személyre (a továbbiakban együttesen felhasználó). Ha a hivatal más személyek (pl: Képviselők) is lehetőséget biztosít bármely informatikai rendszerének használatára, akkor rá nézve is kötelező a szabályzatban foglaltak betartása.

A Szabályzat **területi, tárgyi hatálya** kiterjed minden olyan épületre, helyiségre, ahol a tárgyi hatály alá eső eszközök megtalálhatók, illetve a tárgyi hatály alá tartozó tevékenységeket végeznek. Így a Hivatal tevékenysége során keletkezett, kezelt, feldolgozott, tárolt adatokra és információkra, a számítástechnikai eszközbázisra, ezek okmányaira, leírására és felhasználási környezetükre, a szoftverekre, adatbázisokra és a kapcsolódó dokumentációkra, az adatbiztonsági nyilvántartásokra.

Jelen szabályzatban foglalt elvárások és követelmények a jegyző jóváhagyásával kerültek kialakításra. Azon biztonsági területek esetében, melyeket jelen szabályzat nem fed le, vagy részletesen nem szabályoz, a jegyző határozza meg a követendő eljárásrendet és az

Készítette: Maxentrop Kft.

alkalmazandó biztonsági elvárásokat, melyek meghatározásához szükség esetén bevonja az elektronikus információs rendszerek biztonságáért felelős személyt.

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

1.3 A dokumentum minősítése, kötelezettségek

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

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

1.4 Alapfogalmak

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

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

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

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

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

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

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

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

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

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

Készítette: Maxentrop Kft.

10. biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;
11. biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;
12. biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
13. biztonsági szint: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
14. biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
- 14a. EGT-állam: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) meghatározott állam;
- 14b. elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;
15. elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;
16. életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
17. észlelés: a biztonsági esemény bekövetkezésének felismerése;
18. felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre;
19. fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;
20. fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;
21. folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
22. globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;
23. információ: bizonyos tényekről, tárgyakra vagy jelenségekre hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkentő vagy megszüntető;
24. kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a

Készítette: Maxentrop Kft.

kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

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

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

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

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

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

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

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

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

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

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

35. megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

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

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

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

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

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

Készítette: Maxentrop Kft.

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

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

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

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

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

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

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

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

1.5 Kapcsolódó dokumentumok

Jogszabályok

- a) a munka törvénykönyvéről szóló 2012. évi I. törvény
- b) a büntető Törvénykönyvről szóló 2012. évi C. törvény
- c) a polgári Törvénykönyvről szóló 2013. évi V. törvény
- d) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: lbtv.)
- e) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről (továbbiakban: technológiai vhr) szóló 41/2015. (VII. 15.) BM rendelet
- f) az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet
- g) a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 187/2015. (VII. 13.) rendelet

Készítette: Maxentrop Kft.

- h) h) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet
- i) az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.) szóló 2011. évi CXII. törvény
- j) a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény
- k) a közokiratokról, a közlevéltárakról, és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény
- l) a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról szóló 1999. évi LXXII. törvény
- m) a szerzői jogról szóló 1999. évi LXXVI. törvény
- n) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény.
- o) a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról szóló 1993/146. (X. 26.) Korm. rendelet
- p) 466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézással összefüggő adatok biztonságát szolgáló Kormányzati Adattrezzorról

Kapcsolódó szabványok, ajánlások

- a) MSZ ISO/IEC 27002:2011: Az információbiztonság irányítási gyakorlatának kézikönyve
- b) MSZ ISO/IEC 27001:2006: Az információbiztonság irányítási rendszerei. Követelmények
- c) A KIB 25. számú ajánlása: Magyar Információbiztonsági Ajánlások (MIBA) 1.0 verzió
- d) A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások
- e) A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár

Kapcsolódó szabályozások (többek között)

- f) Számlatükör
- g) Számlarend
- h) Leltározási és leltárkészítési szabályzat
- i) Felesleges vagyontárgyak hasznosításának, selejtezésének szabályzata
- j) Eszközök és források értékelési szabályzata
- k) Önköltség-számítási szabályzat
- l) Pénzkezelési szabályzat

Készítette: Maxentrop Kft.

m) Iratkezelési szabályzat

n) Mentési archiválási szabályzat

1.6 Szerepkörök

A Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata a részletes hivatali szerepköröket a Szervezeti és Működési Szabályzatban rögzítette.

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata (vezető): az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, határoz meg a cselekvési terv teljesülése érdekében.

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

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

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

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

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

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

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

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

g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

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

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

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

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

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

Készítette: Maxentrop Kft.

m) elelnőrzi a védelmi eszközökkel való ellátottságot

n) előzetes bejelentési kötelezettség nélkül ellenőrizheti az informatika, információbiztonsági folyamatok bármely részét

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

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

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

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

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

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

A *rendszergazda* (informatikai rendszerek felügyeletével, kezelésével megbízott személy vagy szervezet) a jegyző iránymutatásának a szerződésben leírtaknak és e szabályzatnak megfelelően végzi feladatait. Szorosan együttműködik az elektronikus információs rendszer biztonságáért felelős személlyel az informatikai biztonsági követelmények kialakításában és végrehajtásában. A védelem helyi operatív végrehajtásáért felelős a rendszergazda.

A rendszergazda feladata:

- a hálózati struktúra tervezése, az új elemek becsatlakozásának szabályozása,

Készítette: Maxentrop Kft.

- hálózaton működő alkalmazások telepítésének tervezése, telepítése vagy a telepítés szakmai felügyelete, használatuk szabályozása,
- a hálózati forgalom figyelése,
- a hálózati hibák felderítése, az elhárításhoz szükséges intézkedések megtétele,
- a hálózati felhasználók üzemeltetési feladatainak szakmai irányítása.
- a hivatali szintű informatikai alkalmazások felügyelete, folyamatos működésük biztosítása,
- az alkalmazás használatához szükséges hálózati- és erőforrás-hozzáférési jogok biztosítása a felhasználók részére,
- az alkalmazásokkal kapcsolatos, felhasználóktól érkező észrevételek fogadása, a szükséges változtatások, módosítások megtétele, regisztrálása,
- a hálózati struktúra nyilvántartása,
- a felhasználók nyilvántartása és tájékoztatása,
- felhasználói programok havi és rendkívüli frissítése,
- új hardver kiegészítők illesztése a már meglévő konfigurációkhoz,
- hardver változtatások végrehajtása hibajavítás vagy elavulás esetében,
- hardver, szoftver nyilvántartási adatok folyamatos frissítése,
- a felhasználók betanításában való közreműködés,
- felhasználói dokumentációk biztosítása,
- az informatikai alkalmazások felügyelete, folyamatos működésének biztosítása.
- a Hivatal informatikai igényeinek (hibák, változások) fogadása, informatikai hibák javítása, informatikai változási igények végrehajtása;
- mentési és naplózási elvárások érvényre juttatása;
- ügyviteli igényeknek megfelelő mentési rend kialakítása és mentési eljárások kidolgozása;
- hatáskörébe tartozó informatikai rendszerek jogosultságadminisztrációs feladatainak ellátása, jogosultság nyilvántartás naprakészen tartása
- a Hivatal elektronikus információs rendszereinek nyilvántartása, beleértve a hardver-, szoftver- és licenccnyilvántartás elkészítését
- részvétel az informatikai biztonsági stratégia felülvizsgálatában, megvalósításában
- új elektronikus információs rendszer bevezetése esetén a felhasználók oktatása
- a Hivatal elektronikus információs rendszereivel kapcsolatos nyilvántartásainak évenkénti felülvizsgálata
- a saját feladatkörébe tartozó rendszerek felügyelete
- felelős az infoematikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és azok karbantartásáért
- gondoskodik a rendszer kritikus részeinek meghatározásáért és újra indíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról
- feladata a védelmi eszközök működésének folyamatos elelnőrzése
- felelős a Hivatali rendszerek hardver eszközeinek karbantartásáért
- gondoskodik a folyamatos vírusvédelem fenntartásáról
- folyamatosan figyelemmel kíséri és vizsgálja a rendszerek működése és biztonsága szempontjából lényeges paraméterek alakulását, kritikus eseményekkor jelzi a Hivatal vezetőjének ellenőrzi a rendszerek adminisztrációját

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

A Hivatali szerepköröket a Hivatal a munkaköri leírásokban, a Hivatal Szervezeti és Működési Szabályzatában – ügyrendjében rögzítette.

A felhasználó:

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

A felhasználónak joga van

- tájékoztatást kapni a helyi felhasználói szabályokról, a rendszergazda személyéről, feladat- és hatásköréről,
- panaszt tenni a rendszergazda intézkedései ellen az adott szervezeti egység vezető-jénél,
- a számára megítélt erőforrások biztosítását a rendszergazdától kérni,
- a géphez hozzárendelt szolgáltatásokat a felhasználói kategóriába sorolástól függően igénybe venni.

A felhasználó kötelessége

- a felhasználókra vonatkozó szabályok betartása,
- a rendszergazda üzemeltetés tárgykörében tett javaslatainak végrehajtása,
- a gép használatával kapcsolatos fontosabb események, hibák bejelentése a rendszergazdának,
- más felhasználók figyelmeztetése a szabályok betartására, a nem rendeltetésszerű, illetve szabályzatokkal ellentétes használat megakadályozása és jelentése,
- az általa felfedezett biztonsági problémák jelentése a rendszergazdának.

A felhasználónak TILOS

- a gépek megbontása, a hardver konfigurációk megváltoztatása,
- az esetlegesen előforduló biztonsági lyukak, hiányosságok kihasználása,
- más felhasználók munkájának zavarása, anyagainak illetéktelen megtekintése, másolása,
- más felhasználó bejelentkezési nevének, illetve jelszavának használata,
- a hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása,
- külső forrásból származó hordozható adattárolók felhasználása a rendszergazda által végzett vírus-ellenőrzés előtt.

Készítette: Maxentrop Kft.

Vírusfertőzés (vagy annak gyanúja) esetén a rendszergazdát azonnal értesíteni kell a gépet le kell kapcsolni, s további használatát a rendszergazda intézkedéséig fel kell függeszteni.

Meghibásodás esetén a hiba kijavítását a felhasználó nem kísérelheti meg, azonban meg kell tennie mindazokat a feladatkörén belül eső intézkedéseket, amelyekkel a hálózatot (adatok, gépek) további károsodástól megóvjá. Célszerű a géppel való munkát azonnal felfüggeszteni és haladéktalanul értesíteni a rendszergazdát.

A felhasználó nem kísérelheti meg a számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzését. Az erre irányuló próbálkozás, annak sikerétől függetlenül, fegyelmi vétségnek minősül.

Amennyiben a felhasználó a szabályzatokban foglaltakat vétkezen – szándékosan vagy gondatlanul – megszegi és személyével kapcsolatosan fegyelmi vétség gyanúja merül fel, a rendszergazda a kötelezettszegésről és annak körülményeiről haladéktalanul írásban tájékoztatja a munkáltatói jogkör gyakorlóját, aki dönt a fegyelmi eljárás megindításáról.

A fegyelmi eljárás lefolytatására, illetve a köztisztviselő kártérítési felelősségének megállapítására a közszolgálati tisztviselők jogállásáról szóló törvény szabályai az irányadók.

A nem köztisztviselő általi károkozás esetén a kárigény érvényesítése a polgári jog általános szabályai szerint történik.

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

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

1.7 Tevékenységek

A Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata a tv.-ben meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

1.8 Hivatalrendszer belső együttműködése

A Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata a belső együttműködését a Szervezeti és Működési Szabályzatban rögzítette.

2 Hivatal besorolási Nyilatkozata

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata nyilatkozatban rögzíti, hogy a Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával a NEIH által kiadott 41 2015 BM VHR SZVI 2.00.xlsm ürlap felhasználásával egy kockázatértékelés során végzett a 2013 évi L tv. 9. §-nak való megfelelés szerinti vizsgálat eredményeként a Hivatal biztonsági szintje a 2013 évi L tv. 9. §. (2) d):

2-es (azaz kettes) besorolású

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

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

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

- 2.1.5. a folyamatokat és végrehajtásukat a Hivatal úgy dokumentálja, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi köre - megállapítható legyen.

3 Rendszerek besorolási nyilatkozata

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata nyilatkozatban rögzíti, hogy a Hivatal szakemberi által biztosított adatok alapján, külsős szakember bevonásával egy kockázatértékelés során végzett 2013. évi L. törvénynek és a 41/2015. (VII. 15.) BM rendeletnek való megfelelés a [NEIH-OVI] Osztályba sorolás és védelmi intézkedések úrlapja (v4.60, MS Office) a 41/2015. (VII. 15.) BM rendelet alapján felhasználásával végzett vizsgálatának eredményeként a Hivatal rendszereinek biztonsági osztályai a következők:

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

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

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

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

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

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

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

Készítette: Maxentrop Kft.

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

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

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

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

Jelen szabályzat csak a rendszerek 2-es szinthez rendelt kötelezettségeket, elvárásokat taglalja. A 2-es szintnél magasabb a Hatóságok által meghatározott védelmi szintnek való megfelelést a Hivatal hatályos Informatikabiztonsági szabályzatának 2. sz. függeléke (Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatika Biztonsági Szabályzat kiegészítése az ASP rendszerek informatikai biztonsági követelményekről) írja le.

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

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

4 Adminisztratív Védelmi Intézkedések

4.4 Szervezeti szintű alapfeladatok

4.5 Informatikai biztonsági szabályzat

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

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

4.6 Az elektronikus információs rendszerek biztonságáért felelős személy

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

4.7 Intézkedési terv és mérföldkövei

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

4.8 Az elektronikus információs rendszerek nyilvántartása

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

- a) a rendszerek alapadatait;
- b) a rendszerek által biztosítandó szolgáltatásokat;
- c) az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett Hivatal kezelésében vannak);

Készítette: Maxentrop Kft.

- d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
- e) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

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

4.6 Rendszer és szolgáltatás beszerzés

Külső elektronikus információs rendszerek szolgáltatásai

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

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

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

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

4.7 Üzletmenet- (ügymenet-) folytonosság tervezése

Üzletmenet-folytonosságra vonatkozó eljárásrend

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

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

Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

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

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

Készítette: Maxentrop Kft.

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

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

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

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

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

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

Biztonsági eseménykezelési terv

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

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

A Jegyző – szükség szerint az IT üzemeltetővel, és az információbiztonsági felelőssel konzultálva – a bekövetkezett kieséses, állapot körülményeiről és hatásairól, becsült időtartamáról

Készítette: Maxentrop Kft.

(helyreállítási idő) rendelkezésre álló információk mérlegelését követően dönt az esemény kezelési módjáról, amely lehet:

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

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

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

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

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

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

4.8 Az elektronikus információs rendszer mentései

Általános követelmények

Az adatok mentése azt a célt szolgálja, hogy üzemzavar esetén az aktuális vagy ahhoz közelálló állapot visszaállítható legyen.

A munkaállomáson tárolt adatok mentését a rendszergazda végzi.

Archiválendő felhasználói dokumentumok mentése a mentési szabályzat alapján történik.

Szervizelés megkezdése előtt a rendszergazda feladata a számítógépek teljes adatmentését elvégezni (amennyiben lehetséges).

Az adatok archiválásnak célja, hogy az adatok valamely állapotának hosszabb távú megőrzését biztosítsa.

Az adatok archiválását a rendszergazda végzi.

Az adatok visszaállítása, katasztrófaelhárítás

A vészhelyzetekből eredő veszteségek csökkentéséhez szükséges, hogy a számítógépes infrastruktúra bármely elemének károsodása esetére "készenlétben álljon" az alkalmazandó megoldás.

Az adatok visszaállítása történhet valamely vészhelyzetben, a számítógép olyan szintű meghibásodásakor, hogy a rajta tárolt információk már nem másolhatóak új gépre, továbbá az adatrendszer sérülése vagy egyéni igény alapján (pl. visszavonhatatlan hibás rögzítés).

Az adatrendszer sérülése esetén a rendszergazda a legfrissebb mentés vagy archiválás alapján elvégzi az adatok visszatöltését és az érintett irodák dolgozóit felkéri a mentés utáni adatváltozások rögzítésére.

Munkaállomás meghibásodása esetén a javítás megkezdése előtt, amennyiben lehetséges, teljes adatmentést kell végezni, ezt követi a felhasználóhoz rendelt operációs rendszer és a felhasználói programok telepítése, konfigurálása.

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

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

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

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

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

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

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

A szerverszobában elhelyezett NAS adattároló eszközre történik a mentés az alábbi eljárás szerint:

- napi mentések: hétfőtől - péntekig; változás mentés 00.00-01.00 között
- heti mentések: szombatonként automatizált módon;
- éves mentések: tárgy év utolsó munkanapját követő nap.

Készítette: Maxentrop Kft.

A tárgy év utolsó mentésének (az éves mentés) megtörténte után a NAS adattároló eszköz tükör merevlemeze cserélődik, egy új merevlemezre. A mentést tartalmazó HDD a jegyzői titkárságon pánccszekrényben kerül elhelyezésre.

Az adatok mentése, az adathordozók biztonsága

A napi adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott fájlokat naponta, a munka befejezésével AES-256 erősségű jelszóval védett .zip fájlba tömörítve az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba (vagy feltöltheti az erre a célra létrehozott FTP tárhelyre).

(2) A külső, biztonságos másolatokat tartalmazó merevlemez csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszertől, és az adatvédelmi felelős által kijelölt helyre kell elzárni (FTP tárhelyre való feltöltés esetén ez úgy módosul, hogy csak a feltöltés idejére szabad az FTP kapcsolatot élővé tenni, adatfeltöltés után a kapcsolatot meg kell szakítani).

(3) A korábbi adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan a 14 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 13 frissebb adatmentés az állományokról.

A heti adatmentés a következő módon történik

(1) Az adatvédelmi felelős által meghatározott, de általánosságban elmondható, hogy a merevlemezen lévő összes fájlról hetente egyszer teljes körű biztonsági másolatot kell készíteni. Az adathalmazok méretének megfelelően vagy a napi mentésnél már szokásos AES-256 erősségű jelszóval védett .zip fájlba tömörítve, vagy az eredeti állapotban; az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba, a könyvtár nevében utalva arra, hogy heti és teljes körű, minden adatot érintő biztonsági másolatról van szó.

(2) A külső, biztonsági másolatokat tartalmazó merevlemez csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszertől és az adatvédelmi felelős által kijelölt helyre el kell zárni.

(3) A korábbi, heti, teljes körű adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan az 1 hónapnál régebbi biztonsági mentést tartalmazó könyvtárak kerülhetnek törlésre, de csak abban az esetben, ha már létezik 3 frissebb adatmentés az állományokról.

Az éves adatmentés a következő módon történik

A tárgy év utolsó teljes körű biztonsági mentésének megtörténte után, az adatmentés helyének kijelölt külső adattároló eszköz tükör merevlemeze cserélődik egy új merevlemezre. A mentést tartalmazó merevlemez pánccszekrényben kerül elhelyezésre.

Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

(1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az adatvédelmi felelőst.

(2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és az adatvédelmi felelős további utasításági nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.

(3) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

(4) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) haladéktalanul értesíti a Hivatal rendszergazdáját.

Készítette: Maxentrop Kft.

(5) A rendszergazda kéréséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését (senki nem nyúlhat hozzá, még az adatvédelmi felelős sem).

Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni. Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

Feladatok és felelőségek

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

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

A szervezeten tárolt adatok mentéséért a rendszergazda a felelős.

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

Az elektronikus információs rendszer archíválása

Az önkormányzat tevékenységéből adódóan, ha saját rendszerein személyes, hivatali védendő adatokat kezel és dolgoz fel és ebből következően archiválási folyamatot tart fent az elektronikus dokumentumok hosszú távú, biztonságos megőrzése, archiválása céljából, akkor a Hivatal az archiválási tevékenységét a rendeletnek megfelelő Archiválási szabályzata szerint hajtja végre.

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

Az elektronikus információs rendszer helyreállítása és újraindítása

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

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

4.9 Emberi tényezőket figyelembe vevő – személy – biztonság

Eljárás jogviszony megszűnése napján

A jegyző vagy erre jogosult megbízottja .

- a) megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;
- b) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;
- c) visszaveszi az érintett hivatal elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;

Készítette: Maxentrop Kft.

- d) megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és a Hivatali információkhoz;
- e) az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
- f) a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
- g) a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartására megelőző intézkedéseket tesz.

A hozzáférési jogok visszavonása

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

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

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

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

A vagyontárgyak visszaszolgáltatása

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

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

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

A munkakör változásának biztonsági kérdései

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

Fegyelmi intézkedések

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

A fegyelmi eljárást a vonatkozó jogszabályi rendelkezéseknek megfelelően folytatjuk le.

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

A jelentésnek tartalmaznia kell:

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

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

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

Viselkedési szabályok az interneten

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

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

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

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

Készítette: Maxentrop Kft.

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

Az e-mailek ellenőrzése

A Levelezés szabályai:

A szabályozás célja, hogy biztosítsák az elektronikus levelezés zavartalanságát valamint védjék a Hivatal érdekeit. Minden felhasználónak és szervezeti egységnek lehetősége van (felhasználói név@bonyhad.hu) című postafiókot igényelni, és ezt kizárólagosan hivatalos célra használni. A hivatal e szabályokra figyelemmel monitorozhatja a hálózathoz küldött, illetve fogadott levelek tartalmát az adatvédelmi szabályok és ajánlások figyelembevételével.

a. A hivatal hálózatán keresztül küldött vagy fogadott levelek központilag vírus- és kémprogram ellenőrzés történik, ami különböző védelmi és szűri funkciókkal egészül ki.

b. A Hivatal hálózatán keresztül küldött levelek központilag Spam ellenőrzésen esnek át.

Alapelvek

- A levelek nem tartalmazhatnak a hatályos magyar jogszabályokba ütköző tartalmat.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.

Szabályok

- Tilos kéretlen leveleket, hirdetések, kör e-maileket küldeni.
- Tilos kör e-maileket reklám anyagokat tovább küldeni.
- Tilos az e-mail címet olyan kereskedelmi listára feltenni, amelyről a hivatali levelező rendszert e-mail szeméttel (spam) terhelhetik meg.
- Tilos a hivatali e-mail cím magánjellegű felhasználása.
- Tilos a hivatali e-mail címet bármely weboldalon regisztrációhoz felhasználni.
- Tilos ismeretlen vagy gyanúsnak tűnő feladótól érkezett levelek mellékletének megnyitása, vagy továbbítása.
- Tilos nagy méretű file-okat e-mail-ben küldeni mert ez túlzott mértékben terheli a hálózatot vagy esetlegesen blokkolhatja postafiókját. Az ilyen nagy méretű (adatbiztonságot nem sértő!) tartalmat publikus helyen kell elérhetővé tenni. Ha tájékoztatás keretében a munkáltató részletesen meghatározza azokat a címeket, ahonnan e-mail fogadható vagy küldhető és a levelező rendszer magáncélú használatát megtiltja, ezt követően a dolgozó teljes levelezése ellenőrizhetővé válik. A Hivatal az ellenőrzés során betartja a jogviszonyban nem álló harmadik személyek személyes adatainak védelmére vonatkozó jogait.

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

Készítette: Maxentrop Kft.

4.10 Tudatosság és képzés

- A felhasználóknak rendelkezniük kell a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel.
- Biztosítani kell a felhasználók rendszeres információbiztonsági oktatását, tudatosítását, tájékoztatását.
- A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az óvintézkedéseket, valamint az informatikai eszközök helyes használatát, az informatikai biztonságpolitikában előírtakat.
- A felhasználóknak ismerniük kell a biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, hogy ezzel is minimálisra csökkentsék a lehetséges biztonsági kockázatokat, és alá kell írniuk az erről szóló nyilatkozatot.
- Minden felhasználónál tudatosítani kell a biztonsági szabályok megsértésével járó szankciókat, és azokat következetesen be kell tartani.

Képzési eljárásrend

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

A Jegyző:

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

Az IBF:

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

A munkatársak:

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

Biztonságtudatossági képzés

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

A képzésnek kötelezően:

- felhívja a munkatársak figyelmét az informatikai biztonsági szabályzati rendszerben bekövetkezett változásokra
- ismerteti azokat a sebezhetőségeket, melyek a felhasználó nem-biztonságtudatos magatartását használják ki;
- ismerteti az azonosított, súlyosnak minősített szabálysértéseket;

Készítette: Maxentrop Kft.

- felhívja a figyelmet, hogy a megadott súlyos szabálysértések ismételt elkövetése milyen szankciókat von maga után.
- A szabályzatokban, jogszabályokban, szerződésekből előírt követelmények felfrissítése érdekében ismerteti a betartandó szabályokat, kötelezettségeket, egy-egy az oktatásra kijelölt biztonsági terület esetében (pl. hozzáférés védelem témakörében a jelszókezelési szabályok stb.)

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

Alkalmazás előtt

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

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

Belső oktatások, továbbképzés

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

Képzési eljárásrend

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

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

5 Fizikai Védelmi Intézkedések

5.1 Fizikai és környezeti védelem

Fizikai védelmi eljárásrend

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

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

Fizikai belépési engedélyek

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

A jegyző:

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

A fizikai belépés ellenőrzése

A jegyző:

- a) kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
- b) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
- c) gondoskodik a létesítmény információs eszközeinek helyt adó létesítményeibe, eseti jelleggel belépők kíséretéről és figyelemmel követi a tevékenységeket;
- d) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;
- e) meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;
- f) felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

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

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

Alapvető normák, üzemeltetési szabályok

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

A Hivatal épületeinek minden oldalról zárható határfelülettel kell rendelkeznie. Minden munkatárs köteles ellenőrizni a felügyelete alatt álló hivatali helyiség nyílászáróinak megfelelő működését, zárhatóságát. Rendellenesen működő, nem zárható nyílászáró javításáról

Készítette: Maxentrop Kft.

haladéktalanul intézkedni kell, emiatt azt soron kívül jelezni köteles a hibát észlelő vagy arról értesülő munkatárs a Jegyző felé.

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

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

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

A szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzvesélyességi osztályba tartoznak, amely mérsékelt tűzvesélyes üzemet jelent. A szerverszobára vonatkozó tűzvédelem feladatait, sajátos előírásait „A Polgármesteri Hivatal tűzvédelmi szabályzata” tartalmazza.

Vagyonvédelem, fizikai biztonság

- a szerverszobát, irodákat biztonsági zárral kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell;
- a szerverszoba kulcsát a hivatali informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel;
- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni;
- a szerverszobába történő illetéktelen behatolás tényét a jegyzőnek azonnal jelenteni kell;
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők, illetve alkalmazottak használhatják;
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Általános informatikai védelem

- A szerverszobában a hivatali informatikuson, valamint az informatikai rendszer üzemeltetését végző gazdálkodó szervezet munkatársán kívül más nem tartózkodhat. Más személyek benntartózkodását a szervezeti egység vezető engedélyezheti.
- Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát a hivatali informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben. A szerverszoba áramtalanításáért a hivatali informatikus a felelős.
- Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért a hivatali informatikus a felelős.
- A szerverszobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!

Készítette: Maxentrop Kft.

- A szerverszobába égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!
- A szerverszoba takarítását csak a hivatali informatikus felügyelet mellett, legalább havonta egyszer, a kijelölt személyek végezhetik.
- A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a hivatali informatikus és a szervizek szakemberei végezhetnek.
- A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani, illetve az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.
- Adathordozókat csak a hivatali informatikus engedélyével lehet be- és kivinni a szerverszobából.
- Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet.
- A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket.
- Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben az adatvédelmi felelős fegyelmi felelősségre vonást kezdeményezhet

Védelmi előírások

- A számítógépeket csak indítójelszóval lehessen elindítani, az indító jelszót 30 naponta meg kell változtatni; induláskor minden esetben vírus-ellenőrző programot kell elindítani;
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell.
- Az egyes szakági rendszerek felhasználói csak jelszavas azonosítást követően léphetnek be a rendszerbe. A felhasználói névnek és a jelszónak minden esetben egyedinek kell lennie.

Minden esetben a jelszavaknak különbözniük kell.

- A bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel vagy külső programmal is.
- A módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni;
- a teljes anyagról heti mentéseket kell készíteni;
- a teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni és azt meg kell őrizni. Ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény).
- A felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól az épületen kívül, egy tűzbiztos helyen kell tárolni.

Felhasználókra vonatkozó szabályok

Felhasználó lehet, az önkormányzat képviselője, a Hivatal dolgozója (köztisztviselő és egyéb jogviszony keretében foglalkoztatott), illetve egyéb személy, aki felhasználói jogot kért és kapott. A Hivatal tisztviselőitől a felhasználói jogosultság teljes egészében csak a Szabályzatban meghatározott esetekben vonható meg, az alapszolgáltatásokon túl igénybe venni kívánt egyéb szolgáltatásokhoz felhasználói jogot kell kérniük a rendszergazdától, a jegyző engedélyével. Egyéb személy felhasználói jogot csak jegyzői engedéllyel szerezhethet.

Általános felhasználói szabályok

Készítette: Maxentrop Kft.

- A Hivatal tulajdonában vagy használatában levő számítógépes infrastruktúra felhasználója köteles munkáját a Szabályzat szerint végezni.
- A felhasználó a számítógépes infrastruktúrát köteles rendeltetésének megfelelően használni. Így tilos különösen: más felhasználók tevékenységének zavarása, illetéktelen jogosultságok és adatok megszerzése, a szoftverek és a hardver elemek megrongálása, működőképességük veszélyeztetése.
- A felhasználó köteles együttműködni a rendszergazdával, köteles figyelembe venni a megfelelő üzemelés érdekében tett javaslatokat.
- A Szabályzat előírásainak az egyéb, a felhasználó általi vétkes megszegése esetén a szabályszegés – egyéb szankciók mellett – a felhasználásból történő kizárást vonhatja maga után.

A Hivatal épületén kívül

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

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

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

- Utcán, tömegközlekedési eszközön és egyéb nyilvános helyen a Hivatal tulajdonát képező informatikai eszközt – különös tekintettel az adathordozókra – nem szabad felügyelet nélkül hagyni.
- Tilos bekapcsolt és bejelentkezett, de nem zárolt laptopot, vagy egyéb hordozható eszközt felügyelet nélkül hagyni.
- Laptopon, hordozható eszközökön, hordozható adathordozón a feltétlen szükséges minimumra korlátozzuk az érzékeny adatok tárolását, ahol adottak ennek a technikai feltételei az érzékeny adatokat titkosítva tároljuk (ennek egy tipikus módja, ha a laptopokon ki alakításra kerül egy titkosított partíció az érzékeny adatok tárolására)
- Nem szabad nyilvános helyen őrizetlenül hagyni.

Üres íróasztal, tiszta képernyő politika

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

- kötelesek az általuk kezelt adathordozókat csak a használat ideje alatt maguknál tartani;
- kötelesek a papír alapú adathordozók kezelése során az iratkezelési szabályzat előírásait betartani;
- a részükre kiadott biztonsági eszközöket a hatályos szabályozások szellemében, más személyek részére nem adhatják át;
- kötelesek az informatika eszközről kijelentkezni vagy azt zárolni minden esetben, ha a tevékenységet befejezte vagy megszakítja oly módon, hogy az informatikai eszköz felügyelet nélkül marad;
- kötelesek minden esetben a harmadik felek felügyeletéről gondoskodni, annak érdekében, hogy az ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz;

Készítette: Maxentrop Kft.

- kötelesek a munkanap végén a rendelkezésére bocsátott informatikai eszközök kikapcsolni. Ez alól a szabály alól a jegyző személyre, eszközre, munkafolyamatra vonatkozó felmentést adhat, ha ez szakmailag indokolt.
- a Hivatal épületén belül, Hivatali informatikai eszközök harmadik személynek csak indokolt esetben lehet átadni (pl. laptop, előadás céljára), de ebben az esetben is gondoskodni kell róla, hogy illetéktelen ne juthasson érzékeny adatokhoz.
- Az ügyfelek, illetve látogatók által látható területen az ügyintézés időtartama alatt a papír alapú adathordozók kezelése során kizárólag az aktuális ügyhöz szükséges iratok lehetnek elő
- kizárólag az aktuális ügyintézéshez szükséges alkalmazások, programablakok lehetnek megnyitva, (amennyiben az ügyfél rálát a képernyőre) a képernyőn.

Látogató kíséréte

Az irodahelyiségekben harmadik személy nem tartózkodhat felügyelet nélkül, az üres irodákat be kell zárni, annak érdekében, hogy ellenőrizetlenül senki ne férjen hozzá informatikai eszközökhöz vagy egyéb adathordozóhoz.

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

Számítógépek, szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen és maradéktalanul elvégezni:

- menteni a még használható fizikai és logikai eszközöket
- biztonsági mentésekből, háttértárról a megsérült adatok visszaállítása
- archivált anyagok (ill. tartalék eszközök) használatával folytatni kell a feldolgozást

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése, tartalékolása. Az üzemeltetést, karbantartást és szervizelést a rendszergazda végzi. Információs eszköz megbontását (kivéve garancia) csak a rendszergazda végezheti el. A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlásait,
- mások és a saját tapasztalatot

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót. A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

Informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme:

- adatbevitel hibátlan állapotú eszközön történhet
- csak tesztelt, leltárban lévő adathordozóra lehet adatokat másolni, rögzíteni
- a jogosultságok használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz,
- az adatok bevitelénél elv, hogy azonos állomány rögzítését és ellenőrzését ugyan az a személy nem végezheti,

Készítette: Maxentrop Kft.

- az adatrögzítési dokumentumok:
 - o adatrögzítési utasítások
 - o ellenőrzési utasítások
 - o programok kezelési utasításai
 - o megőrzési és archiválási utasítások
 - o kezelési és karbantartási utasítások.

Központi gépek védelme

Szünetmentes áramforrást kell használni, amely megvédi az információs eszközt a feszültségingadozásoktól, adatvesztéstől, egy áramkimaradás esetén. A központi gépek háttértáiról folyamatosan biztonsági mentést kell végezni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

Munkaállomások gépeinek a védelme

Külső helyről hozott, kapott adatokat a használat előtt, egy arra alkalmas (hálózatról leválasztott) gépen, a rendszergazda által, vírusellenőrző programmal kell ellenőrizni. Új rendszerek használata előtt, szükség szerint adaptálni kell és tesztadatokkal ellenőrizni kell a működésüket.

A hálózati elemek és vezetékek, csatlakozók és egyéb átviteli elemeket mindennemű sérüléstől óvni kell. Ezek illetéktelen megbontása tilos.

6 Logikai Védelmi Intézkedések

Általános védelmi intézkedések

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

A Hivatal rövid topológiája: A Hivatalban található kliens számítógépek csavart érpáras UTP kapcsolattal csatlakoznak a helyi szerverhez. A PC-k és a központi szerver közötti hálózati kapcsolatot Windows 2000 kompatibilis hálózati szoftver biztosítja. A Polgármesteri Hivatal optikai kapcsolaton csatlakozik az Internethez, melynek sebessége 10/10 Mbit/sec. A hálózaton központi szerver üzemel, amely 40 PC számára biztosítja az adatbázisok elérését.

Személyi biztonság

A jegyző:

- a) megfogalmazza, dokumentálja, valamint kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;
- b) Az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;
- c) legalább évente felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat a

Készítette: Maxentrop Kft.

rájuk vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását;

- d) gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;
- e) meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket;

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

6.1 Tervezés

Rendszerbiztonsági terv

A Jegyző a saját működtetésű elektronikus információs rendszereihez jelen dokumentumban rendszerbiztonsági tervet készít, amely:

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

Cselekvési terv

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

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

Készítette: Maxentrop Kft.

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

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

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

Személyi biztonság

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

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

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

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

meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket

6.1 RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

Általános szabályok

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

Hardver beszerzés

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

Szoftver beszerzés

Készítette: Maxentrop Kft.

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

A Hivatal számítógépes rendszerében csak legális, jogtiszt szoftverek üzemeltethetőek. További követelmény, hogy a szoftverek integráltan, összehangoltan működjenek. Ezen célok biztosítása érdekében új szoftverek beszerzése kizárólag a rendszergazda véleménye után lehetséges. A beszerzések során az alábbiak megtartása szükséges.

Források

A szoftverek beszerzésére fordítható összegeket a Hivatal költségvetése szabja meg. Az egyes szervezeti egységek igényeiket a jegyző felé a költségvetés összeállítása előtt jelzik. A rendszergazda feladata a szükségszerű cserékről, frissítésekről a jegyzővel konzultálni.

A rendszergazda véleményezi a beszerezni kívánt szoftver igényeket, véleménye a szoftver tartalmára és árára egyaránt vonatkozik.

Szoftverek kiválasztása

A szoftverek kiválasztására szóló javaslatétel a rendszergazda feladatkörébe tartozik. A különböző felhasználói igények megfelelő szintű kielégítése érdekében a megfelelő alkalmazói szoftver kiválasztása előtt a rendszergazda konzultál az igénylő iroda szakembereivel.

Beszerzési módok

A kiválasztott szoftverek beszerzése a jegyző hatásköre.

Szoftver vásárlás

Szoftver vásárlása csak közvetlenül a szoftver gyártótól, vagy annak hivatalos viszonteladójától történhet. A vásárlásnál figyelembe kell venni a tervezett felhasználói számot. A szoftvert a megfelelő számú felhasználói licensszel együtt kell megvásárolni, illetve regisztráltatni.

Külső fejlesztés (outsourcing)

Külső fejlesztést csak fejlesztési szerződés alapján lehet végeztetni. A szerződésnek pontos specifikációt és ütemtervet kell tartalmaznia.

Szoftverek telepítése

Szoftver-telepítését csak a rendszergazda, szerződés alapján a beszállító, illetve meghibásodás esetén a karbantartásra szerződött cég végezhet. Ez egyaránt vonatkozik hálózatos szoftverek esetén a szerverre történő telepítésre és a felhasználókhöz való installálásra is.

Jogvédelem

A Hivatal rendszerébe, akár hálózatra, akár önálló gépre, csak legálisan beszerzett, jogtiszt szoftver telepíthető, illetve ezen eszközökön csak legálisan beszerzett, jogtiszt szoftverek tarthatóak. Ennek központi ellenőrzéséről a rendszergazda gondoskodik.

Szoftverek üzemeltetése

A szoftverek üzemeltetési feladatait a rendszergazda látja el. Ez folyamatos tevékenységet igénylő feladat, mind a szoftverkövetés, rendszeres mentés, mind pedig a rendszerhasználat felügyelete, ellenőrzése.

A rendszergazda feladata a felhasználók rendelkezésére állás azok szoftver kezelési, szoftver működési problémáival kapcsolatban. A szoftverek kezelési problémáira helyszíni vagy telefonos segítségnyújtással, dokumentációkkal adhat megoldást.

A felhasználók problémáik megoldását a rendszergazdától közvetlenül kérhetik. A rendszerfelügyelet célja a rendeltetésszerű használat ellenőrzése, biztosítása. Ebbe beletartozik

Készítette: Maxentrop Kft.

az illegális szoftver- ill. rendszerhasználatok kiderítése és megakadályozása, a vírusfertőzések ellenőrzése, jelentése és megszüntetése éppúgy, mint a nem használt szoftverelemek behatárolása, kivonásukra vagy kiváltásukra történő javaslattétel.

Kellékanyag beszerzés

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

6.2 A rendszer fejlesztési életciklusa

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

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

A jegyző a saját működtetésű elektronikus információs rendszerhez meghatározza és a Hivatalra érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

A rendszer életciklus szakaszai a következők:

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

6.3 Konfigurációkezelés

Konfigurációkezelési eljárásrend

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

Elektronikus információs rendszerek nyilvántartása

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

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

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

Elektronikus információs rendszerelem leltár

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

A nyilvántartásunk kiterjed:

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

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

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni. A vonatkozó számviteli tv. szerint a leltári adatokat 10 évig meg kell őrizni. A bizonylat elektronikus formában is megőrizhető, ha biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos olvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

Alapkonfigurációs nyilvántartás

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

A nyilvántartásnak legalább az alábbi tételeket kell tartalmaznia:

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

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

A szoftverhasználat korlátozásai

A jegyző:

- a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt engedélyez, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;
- b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
- c) ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.
- d) ellenőrzi, hogy a Hivatal eszközein szoftvereket (beleértve a hozzájuk tartozó dokumentációt) csak a felhasználási jog keretei szerint szabad telepíteni, másolni, futtatni, kivéve a törvény adta szabad felhasználás körében (így különösen biztonsági másolat készítése céljából). Egyetlen termék többszörös használata esetén a szoftver

Készítette: Maxentrop Kft.

csak a licenc megállapodásnak megfelelően használható. A Hivatal informatikai eszközeire TILOS illegális és/vagy nem jogtiszt szoftvert telepíteni!

- e) engedélyével a Hivatal informatikai eszközeire szoftvereket a felhasználó is telepíthet, de tudatában kell lennie annak a informatikai biztonsági kockázataival.
- f) által átruházott az informatikai rendszerek üzemeltetési feladataival megbízottak felelőssége, hogy csak akkor telepítsenek licencköteles programot informatikai rendszerre, ha előzetesen meggyőződtek róla, hogy azzal szerzői jogot, licenc megállapodást nem sértenek, a program jogszerű használatát igazoló bizonylatok, okiratok rendelkezésre állnak.
- g) által megbízott rendszergazda feladata rendszeres időközönként (legalább kétévente) ellenőrizni automatikus, vagy manuális módszerekkel a hivatali szoftverhasználat jogtisztaságát, illetve szerzői jogvédett tartalmak (pl. zene, film, dokumentumok) jogosulatlan megosztását a Hivatal informatikai rendszerein.
- h) illegális szoftverek használata, illetve a Hivatal által nem engedélyezett szerzői jogvédett tartalmak tárolása esetén a használatban és megosztásban érintett felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat, mely eljárást az informatikai feladatokért felelős vezető kezdeményezheti.

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetőek legyenek az illetékes felhasználók számára.

Rendszerszoftver védelem:

- a rendszerszoftver módosításához az illetékes engedélye szükséges;
- a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni;
- a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni
- (eseménynapló).

Programhoz való hozzáférés, programvédelem:

- A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni.
- Gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek
- A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartania

program dokumentációt.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója;
- a program készítőjének neve;
- a feldolgozási rendszer megnevezése.

Programok megőrzése, nyilvántartása:

- a programokról naprakész nyilvántartást kell vezetni;
- a nyilvántartásból egyértelműen megállapíthatónak kell lennie a program azonosítására és kezelésére vonatkozó adatok.

Készítette: Maxentrop Kft.

Programok fizikai védelme:

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni.

Rendszerszoftver

Az üzemeltetésért felelős informatikusnak biztosítani kell, hogy a rendszerszoftver napra-kész állapotban legyen és a segédprogramok programkönyvtárak mindig hozzáférhetőek legyenek a felhasználók számára.

Felhasználói programok

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen pró-bálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne káro-sodjanak, a követelményeknek megfelelően működjenek:

Bejelentkezési biztonság (LOGIN SECURITY)

A Hivatalban dolgozók felhasználói jogosultságát és annak körét a rendszergazda a felhasználó nyilvántartásban vezeti. A nyilvántartás vezetése és folyamatos aktualizálása a rendszergazda feladata.

A Hivatal az elektronikus információbiztonsággal, rendszer- és szoftverhasználattal kapcsolatos szabályait egy külön dokumentumban (*Engedélyezési és jogosultsági szabályzat*) kezeli.

A felhasználó által telepített szoftverek

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

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

6.5 Karbantartás

Rendszer karbantartási eljárásrend

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

Rendszeres karbantartás

A jegyző által megbízott személyek vagy vállalkozók:

- a) a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
- b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
- c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;

Készítette: Maxentrop Kft.

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

Tervezett karbantartások

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

Számítógépek és szerverek: évenkénti karbantartás

Számítástechnikai hálózat: évenkénti karbantartás és tesztelés

Nyomtatók és egy eszközök: igény szerinti, de legalább évente

Hardver védelem:

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigény bevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a szerverszobában klímaberendezés használata ajánlott; szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerverszobában kell elhelyezni;
- a számítógép-hálózat csatornáit lehetőség szerint külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát;
- a fali csatlakozók megbontása szigorúan tilos;
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez;
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni;
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember (hivatali informatikus), illetve a szervizek szakemberei nyúlhatnak bele;
- havi rendszerességgel a számítógépeken hardver tesztekkel kell lefuttatni.
- számítógépek, perifériák, nyomtatók meghibásodása vagy felhasználó váltása esetén, illetve 1 év folyamatos üzemelés után az alapvető karbantartást el kell végezni (felület tisztítása, az eszköz belsejéből a por eltávolítása, érintkezők tisztítása),
- az informatikai rendszereket kiszolgáló szerverek karbantartását évente el kell végezni (tisztítás, portalanítás stb.),
- a működéshez szükséges hálózati kiszolgáló eszközök (switch, router) meghibásodása esetén azokat a tartalék készletből azonnal pótolni kell.

Készítette: Maxentrop Kft.

Szoftverek karbantartása

- a rendszergazda köteles a használt szoftverek frissítéseit figyelemmel kíséreni, a kritikus frissítéseket haladéktalanul telepíteni,
- az üzemeltetett informatikai rendszerek verzióváltásait annak rendelkezésre állása után azonnal telepíteni kell,
- rendszergazda folyamatosan ellenőrzi, hogy minden használt szoftver üzemeltetési feltételei biztosítottak-e (szükséges memória mennyiség, tárterület).

Az elvégzett karbantartási munkákat a karbantartási naplóban rögzíteni kell.

Adathordozók védelmére vonatkozó eljárásrend

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

- a) hozzájárul az adathordozók kezeléséből eredő kockázatok csökkentéséhez;
- b) lehetővé teszi valamennyi, a tevékenységet érintő adathordozók kezelésével kapcsolatos fenyegető esemény azonosítását;
- c) könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak, illetve rendelkezésre álljanak,
- d) a jogosultság és a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- e) a használt adathordozókat a használat után a tárolási helyre kell visszatenni,
- f) munkaidőben a munkaasztalon, csak az aktuális adatfeldolgozáshoz szükséges adathordozók lehetnek
- g) adathordozót nem jogosultnak, csak a Jegyző utasítására lehet átadni,

Vagyontárgyakért viselt felelősség

- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni;
- az adathordozók nyilvántartásában az azonosító adaton kívül a felírás és megőrzés dátumát, a védetség tényét, a jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni;
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet;
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg;
- az adathordozókat félévenként ellenőrizni és tisztítani kell;
- épületen kívülre vitt adathordozót (laptop is) titkosítani kell.
- csak a Hivatal által biztosított adathordozót lehet használni a hivatali munka során.

Az olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő:

- a) a fizikailag sérült, javíthatatlan;

Készítette: Maxentrop Kft.

- b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott);
- c) ha a kapacitás a névleges érték 75%-ánál kevesebb;
- d) véglegesen elhasználódott adathordozót.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell lelet-tározni.

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

Adathordozók védelme

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

Hozzáférés adathordozókhoz

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

A használni kívánt adattárolót a tárolásra kijelölt helyről vesszük ki és használatot követően oda is helyezzük vissza. A munkaasztalokon csak a munkavégzéshez használatos adathordozók lehetnek.

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

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

Adathordozók törlése

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

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

Informatikai nyilvántartások

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

Készítette: Maxentrop Kft.

Adathordozók használata

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

6.6 Azonosítás és hitelesítés

Azonosítási és hitelesítési eljárásrend

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

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

Azonosító kezelés

A jegyző:

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

A hitelesítésre szolgáló eszközök kezelése

A Jegyző által kijelölt személy:

- a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
- b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
- c) biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
- d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
- e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
- f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
- h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
- i) megköveteli a hitelesítésre szolgáló eszközök felhasználoitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
- j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

A hitelesítésre szolgáló eszköz visszacsatolása

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

Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

A Hivatal hálózatának távoli elérésére az egyes munkaállomások távoli elérésének keretében van lehetőség (titkosított terminál kapcsolat).

A távoli elérések szabályai:

- A bejelentkezés időtartamára a felhasználóra kötelezőek a jelen szabályzatban foglaltak
- A távoli elérésnek biztonságos titkosított terminál kapcsolaton keresztül kell megvalósulnia
- A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító/jelszó megadása)
- a belépési azonosítókat másra átruházni, illetve más azonosítóját használni tilos
- 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani
- a bejelentkezéseket naplózni kell a tűzfalon. A naplózás beállításáért a hálózatért felelős rendszergazda felel

6.7 Hozzáférés ellenőrzése

Hozzáférés ellenőrzési eljárásrend

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

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

Felhasználói fiókok kezelése

A jegyző:

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

...értesíti a fiókkezelőket, ha:

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

...feljogosít az elektronikus információs rendszerhez való hozzáférésre:

- a) az érvényes hozzáférési engedély,

Készítette: Maxentrop Kft.

- b) a tervezett rendszerhasználat,
- c) az alapfeladatok és funkcióik alapján;

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

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

Hozzáférés ellenőrzés érvényesítése

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

A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mivel egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a tulajdonosára, hanem a Hivatal informatikai rendszerére is negatív következményekkel járhat.

Alapelvek:

- Nem szabad könnyen kitalálható jelszavakat választani. A jelszavakat titokban kell tartani
- Az induló jelszót első bejelentkezéskor meg kell változtatni. Ha a felhasználónak gyanúja támad, hogy a jelszava kompromittálódott, azonnal meg kell változtatnia
- A jelszavakat nem szabad kódolatlanul tárolni

Helyes jelszóválasztás:

- nem szabad könnyen kitalálható, személyre jellemző jelszavakat használni
- nem szabad sorozatokat használni (pl abcdefg, 7654321 stb)
- kerülni kell a szótári szavak használatát
- a jelszó tartalmazzon kis és nagybetűket, számokat

Jelszóvédelem

A felhasználóknak különös figyelmet kell, hogy fordítsanak az alábbiakra:

- a jelszót tilos másoknak elmondani, mások előtt a jelszóról beszélni
- a jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti
- tilos közös jelszavakat használni
- a jelszót nem szabad elérhető helyen tárolni, telefonon, e-mailben továbbítani
- a jelszót tilos kérdőívbe, űrlapokba beírni

A felhasználóknak különös figyelmet kell, hogy fordítsanak az alábbiakra:

- A jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti.
- A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
- Tilos közös jelszavakat használni.
- A jelszót nem szabad leírni és hozzáférhető helyen tárolni.
- A jelszót nem szabad telefonon vagy e-mailben továbbadni.

Készítette: Maxentrop Kft.

- Ne használjuk a programok (böngészők) jelszó megjegyző funkcióját.
- Jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni a jelszót és értesíteni kell a rendszergazdát.
- A belépéshez szükséges jelszót biztonságos helyen kell tárolni, soha nem szabad azt a számítógép közelében felírva hagyni.
- Olyan jelszót célszerű választani, amit nem könnyű kitalálni, és a jelszót gyakran meg kell változtatni.
- Óvakodni kell attól, hogy mások jelenlétében gépeljük be a jelszót.
- Amikor nincs szükség a számítógépre, ki kell kapcsolni.

Felelősök, dokumentálás

- Azon informatikai rendszerek esetében, melyek támogatják a jelszavakra vonatkozó alapszabályok kikényszerítését a szükséges szabályok, paraméterek, beállításáért a rendszergazda felel. A dokumentáció ebben az esetben az informatikai rendszer napló állománya.
- Azon informatikai rendszerek esetében, melyek nem támogatják a jelszavakra vonatkozó alapszabályok kikényszerítését az e fejezetben meghatározott elvek szabályok betartásáért, valamint a jelszócsere dokumentálásáért a szervezeti egység vezetője a felelős.

Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

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

Külső elektronikus információs rendszerek használata

A jegyző és a külső rendszer működtetője meghatározza, hogy:

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

Nyilvánosan elérhető tartalom

A jegyző:

- a) kijelöli a Hivatal vezető beosztású munkatársát, aki jogosult a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivaltaltól kapcsolatos bármely információ közzétételére. A Hivatalban csak a Jegyző által engedélyezett információkat lehet közzétenni. Minden más információ közzététele TILOS!
- b) a kijelölt személyt képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;
- c) közzététel előtt átvizsgálja a javasolt tartalmat;

Készítette: Maxentrop Kft.

- d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.
- e) A jegyző nyilvánosan elérhető rendszerként definiálja például a Hivatal publikus weboldalát.
- f) A publikus felületeken való közzétételt és a médiával való kommunikációt a jegyző szabályozza, a Hivatal külső kommunikációjáért a jegyző a felelős.
- g) A Hivatali honlap (domain.hu) tartalommenedzsmentjét a egy külsős megbízott, megbízási szerződés keretében végzi.
- h) A hivatali ügyintézésrel kapcsolatos dokumentációk, határozatok, rendeletek a jegyző, illetve a polgármester jóváhagyását követően kerülnek nyilvánosságra.
- i) A publikált információk csak nyilvános adatokat és információkat tartalmazhatnak. A jegyző legalább évente áttekinti a honlapot és nem nyilvános adat kikerülése esetén eltávolítja azt.

Az informatikabiztonsági felelős időszakos ellenőrzés keretében szintén ellenőrzi a honlap jogszabályoknak való megfelelését.

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

6.8 Rendszer- és információsértetlenség

Rendszer- és információsértetlenségére vonatkozó eljárásrend

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

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

Hibajavítás

A jegyző vagy általa megbízott személy:

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

Kártékony kódok elleni védelem

A jegyző vagy általa megbízott személy:

- a) az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat.

- b) frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

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

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

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani. A vírusvédelmi programok adatbázisát naprakészen kell tartani. Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a szervezeti egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

Az elektronikus információs rendszer felügyelete

A jegyző a rendelkezésre álló információbiztonsági eszköz és alkalmazás segítségével:

- a) felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
- b) azonosítja az elektronikus információs rendszer jogosulatlan használatát;

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

A kimeneti információ kezelése és megőrzése

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

6.9 Naplózás és elszámoltathatóság

Naplózási eljárásrend

A jegyző az általa üzemeltetett EIR-ekre vonatkozó az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként, külön dokumentumban határozza meg, az alábbi általános követelmények figyelembevételével:

Naplózható események

- informatikai rendszerek naplózási rendszerének kialakítása (Windows naplófájlok, adatbázisok log fájlok), hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket, ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint illetéktelen hozzáférés megtörténtét,
- a biztonsági napló adatait havonta egy alkalommal a rendszergazdának ellenőrizni kell,
- az esetleges illetéktelen hozzáférést, jogosultságokkal való visszaéléseket - melyek szankciókat vonnak maguk után - jegyzőkönyvben rögzíteni kell,
- a visszaélés tényét a hivatal vezetője felé azonnal jelezni kell,
- a biztonsági naplók és a jegyzőkönyvek archiválандók, adatait védeni kell az illetéktelen hozzáféréstől,
- a naplóállományok megőrzési idejét az iratkezelési szabályzat részeként kell meghatározni.

A jegyző az érintett elektronikus információs rendszerre vonatkozó rendszerbiztonsági tervben:

- a) meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét.
- b) egyeztet a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő Hivatali egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
- c) megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.
- d) A számon kérhetőség és hibakezelés biztosítása érdekében az informatikai eszközöknek az informatikai rendszer működéséről és különösen az informatikai biztonsági eseményekről helyi naplóállományt generál.

Készítette: Maxentrop Kft.

- e) A jegyző felelőssége, hogy a kialakított naplózási rendszer a szükséges mértékben biztosítsa a számon kérhetőséget és az auditálhatóságot, tegye lehetővé a bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel azokra, melyek a rendszer biztonságát érintik.
- f) Ha a jegyző másként nem rendelkezik az informatikai eszközök minimálisan az alapértelmezett naplózási beállítások szerinti eseményeket naplózza. Az adott informatikai eszköz üzemeltetéséért felelős személy, ha azt az üzemeltetési, üzemeltethetőségi szempontok indokolják saját hatáskörben módosíthatja az alapértelmezett naplóbeállításokat, az jegyző tájékoztatása mellett. A naplóállományokat meghibásodás vagy biztonsági incidens esetén, eseti jelleggel vizsgálja. Meghibásodás esetén a naplóállományok vizsgálata a hibajavításban eljáró üzemeltető feladata. A naplóállományok rendszeres átvizsgálása, a rendszerek naplóállományainak mentése, archiválása alapesetben nem elvárás

Naplóbejegyzések tartalma

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

Időbélyegek

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

A napló információk védelme

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

A naplóbejegyzések megőrzése

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

Naplógenerálás

A jegyző a Hivatal által üzemeltetett rendszereknél:

- a) biztosítja a naplóbejegyzés generálási lehetőségét a meghatározott, naplózható eseményekre;
- b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;
- c) naplóbejegyzéseket állít elő a szükséges eseményekre, a meghatározott tartalommal.

A dolgozókat a belépéskor, és az éves oktatás keretében tájékoztatjuk, hogy mit, mikor, hogyan miért, naplózunk. Tájékoztatjuk, hogy ehhez nem kell engedély, csak tájékoztatás. Indokoljuk, hogy a hivatali gépeket, csak hivatali tevékenységre, munkára lehet használni. Továbbá tájékoztatjuk a jogszabályban biztosított jogairól.

Készítette: Maxentrop Kft.

6.10 Rendszer- és kommunikációvédelem

Rendszer- és kommunikációvédelmi eljárásrend

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

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

A hálózat használatának szabályai:

A hivatal hálózata nem használható az alábbi tevékenységekre:

- a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát zavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásokat indokolatlanul igénybe vevő tevékenységek
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítása, megromlása, megsemmisítése, vagy bármely károkozásra irányuló tevékenység
- hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna.

A felhasználók kötelességei:

- a felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködés a hálózat üzemeltetőjével a szabályzat betartása érdekében a felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

A felhasználók jogai:

- Minden hivatali dolgozónak joga van saját felhasználói fiókhöz és levelezéshez (e- mail címhez) és a munkavégzéshez szükséges web szolgáltatáshoz
- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetője tiszteletben tartja, ettől eltérni csak jogszabály által meghatározott esetekben lehet
- A rendszer technikai karbantartásairól tájékoztatni kell a felhasználókat, hogy kellő idő maradjon a felhasználók felkészülésére. A karbantartásokat lehetőleg hivatali munkaidőn kívül kell lebonyolítani.

A felhasználók regisztrálásának szabályai:

- Felhasználó a hivatal, önkormányzat dolgozója lehet.
- A felhasználói azonosítók kiadása központilag a felelős rendszergazda által történik
- A felhasználót az azonosító átadásakor tájékoztatni kell a használat feltételeiről és szabályairól. A tájékoztatást követően a felhasználó aláírásával igazolja, hogy azokat megismerte és magára nézve kötelezőnek ismerte el.
- Szakrendszerhez kapcsolódó felhasználói azonosító átadását megelőzően a felhasználót oktatásban kell részesíteni annak használatáról.
- A felhasználói azonosítót le kell tiltani, ha azzal visszaélés történt és az esetet ki kell vizsgálni

Készítette: Maxentrop Kft.

- A felhasználó azonosítókat a rendszerből törölni kell, ha felhasználó már nem hivatal dolgozója, illetve az adott rendszer használatához már nincs joga. A törlést az érintett szervezeti egység vezetője kezdeményezi a rendszergazdánál

- A rendszergazda a felhasználói azonosítókról és kapcsolódó hozzáférési jogosultságokról teljes körű és naprakész nyilvántartást vezet. A nyilvántartásnak tartalmaznia kell azon felhasználói azonosítókat és kapcsolódó jelszavakat, hozzáférési jogosultságokat, amelyek más, nem a Hivatal rendszeréhez tartoznak, de valamely feladat kapcsán a Hivatal vagy a Hivatal dolgozója hozzáférést igényelt, kapott ahhoz (pl pályázati rendszerhez történő hozzáférés, hivatali kapuhoz történő hozzáférés) A nyilvántartásba vételt az érintett szervezeti egység vezetője írásban kezdeményezi.

A határok védelme

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

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

Kriptográfiai kulcs előállítás és kezelése

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

Kriptográfiai védelem

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

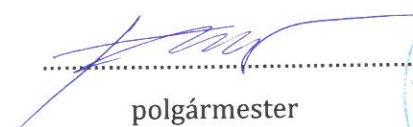
Együttműködésen alapuló számítástechnikai eszközök

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

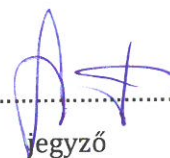
Folyamatok elkülönítése

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

Dátum: 2021. 10. 01


polgármester




jegyző



Készítette: Maxentrop Kft.

Szerzői jogok

Ez a dokumentum a Bonyhádi Közös Önkormányzati Hivatal tulajdona, melyet a Maxentrop Kft. készített el számára. Így a dokumentum szerzői jogaival a Maxentrop Kft. rendelkezik.

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata
INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

1. sz. függeléke

Sorszám:	A rendszer megnevezése:	A rendszer rövid leírása:	A rendszer biztonsági osztálya:	B S R	A rendszer aktuálisan megfelel:
1.	ASZA Anyakönyvi szolgáltató rendszer	Anyakönyvi szolgáltató rendszer. Anyakönyvek és anyakönyvi kivonatok, választási, lakcím, egyéb adatok elektronikus nyilvántartása	2		0
2.	Cím és körzetnyilvántartás	Lakcímnnyilvántartás, új felvitele és meglévő módosítása	2		0
3.	CSTINFO	a családtámogatási ellátásokban (anyasági támogatás, nevelési ellátás-iskoláztatási támogatás (együtt: családi pótlék), gyermekgondozási segély, gyermeknevelési támogatás) részesülők a gyermekek, akikre tekintettel az ellátást megállapították, továbbá a fogyatékosági ellátásban részesülők nyilvántartása	2		0
4.	E-adat	Magyar Államkincstár Területi Igazgatóságok internetes ügyfél tájékoztató portálja. Elektronikus adatforgalmazás	2		0
5.	EAK Elektronikus Anyakönyvi Rendszer	Anyakönyvek nyilvántartása	2		0
6.	EBR 42	Helyi önkormányzatok és Többcéjú Kistérségi Társulások hozzájárulásainak és normatív, kötött felhasználású támogatásainak igénylési, elszámolási rendszere. Pályázati lehetőségek pl. Vis Maior benyújtása	1		0
7.	EPTK PÁLYÁZATI E-ÜGYINTÉZÉS FELÜLET	Pályázatok, hiánypótlások benyújtása	1		0
8.	ÉTDR	Építésügyi hatósági engedélyezési eljárásokat támogató elektronikus dokumentációs rendszer, az egységes hatósági felületen elektronikusan, elektronikus kérelemmel együtt feltöltött, az engedély-kérelmekhez tartozó dokumentációk elektronikus kezelésére, véleményezésére	2		0
9.	Helyi levelező rendszer	Hivatali ügyintézással kapcsolatos levelek	2		0
10.	Hivatali kapu	Földbérlet, föld adás-vétel kifüggesztése, közzététele, kapcsolattartás a felügyeleti szervekkel.	1		0

11.	KCR	Egységes, teljes, közhiteles Központi Címregiszter	2	0
12.	KIR3	Központosított illetményszámfejtési rendszer, dolgozói adminisztrációs rendszer	2	0
13.	KIRA	Központosított illetményszámfejtési rendszer. Foglalkoztatottak, jogviszonyban állók személyi juttatásainak (illetmények, juttatások), egészségbiztosítási ellátások és a munkáltatókat terhelő közterheknek elszámolása.	2	0
14.	Közigállás	Közszféra álláshirdetéseinek nyilvántartása, közzététele	2	0
15.	KSH Elektra	Központi Statisztikai Hivatal adat gyűjtő és adatszolgáltató rendszer	1	0
16.	NJT	Nemzeti rendelet-, jogszabálytár, kapcsolattartás a törvényességi felügyelettel üzenet formájában, rendeletek, jegyzőkönyvek, határozatok felvitele	1	0
17.	Országos kereskedelmi nyilvántartás	Bejelentés-köteles kereskedelmi tevékenységek és üzlet működési engedélyek országos nyilvántartása	2	0
18.	OTP direkt Electra Terminál	Számlák kifizetése, munkabérek utalása, önkormányzati segélyek és támogatások utalása	2	0
19.	Önegm	Önkormányzati előirányzat-gazdálkodási modul, MÁK felé adatközlés. Szociális ellátások igénylése	2	0
20.	PROBONO	Közszolgálati tisztviselői, vezetői képzések nyilvántartása, tervezése	2	0
21.	PTR	Pénzbeni és természetbeni szociális juttatások, ellátások nyilvántartása	2	0
22.	Takarékbank ELEKTRA	Számlák kifizetése, munkabérek utalása, önkormányzati segélyek és támogatások utalása	2	0
23.	Takarnet	Ingatlan tulajdonlapok lekérdező rendszere	2	0
24.	VÁKIR	Választási Kommunikációs és Információs Rendszer. Választási adatok adminisztrálása, lekérdezése	2	0
25.	Winszoc	Szociális juttatások adatainak nyilvántartását kezelő rendszer	2	0
26.	Választási Kapu	Választási alrendszerek elérésének biztosítása (NVR, VÁKIR)	2	0

ASP rendszerek MÁK általi besorolásai.

Sorszám:	A rendszer megnevezése:	A rendszer biztonsági osztálya, megvalósulása esetén:			A rendszer aktuálisan megfelel:
		B	S	R	
27.	Önkormányzati ASP - keretrendszer	4	4	4	0

28.	Önkormányzati ASP - adóügyi rendszer	4	4	4	0
29.	Önkormányzati ASP - gazdálkodási rendszer	3	3	3	0
30.	Önkormányzati ASP – támogató rendszer (hibajegy kezelő)	2	2	2	0
31.	Önkormányzati ASP – hagyaték leletár rendszer	3	3	3	0
32.	Önkormányzati ASP - Ingatlanvagyon-kataszter	3	3	3	0
33.	Önkormányzati ASP – ipar és kereskedelmi rendszer	3	3	3	0
34.	Önkormányzati ASP – iratkezelő rendszer	3	3	3	0
35.	Önkormányzati ASP – anyakönyvi rendszer	4	4	4	0



MAXENTROP KFT

Bonyhádi Közös Önkormányzati Hivatal
és Bonyhád Város Önkormányzata

Informatika Biztonsági Szabályzat
kiegészítése az ASP rendszerek
informatikai biztonsági
követelményekről

Kelt: 2021.10.01.

Általános rész

Cél, a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata által kezelt adatok biztonságának a megteremtése. Továbbá az információbiztonsági követelményeknek való megfelelés biztosítása. E szabályzat kiegészítésnek összhangban van az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel, a hozzátartozó 41/2015. (VII. 15.) BM rendelettel, valamint a 257/2016. (VIII. 31.) Korm. rendelettel.

További cél, hogy a szabályzat egységes szerkezetbe foglalja a Hivatal által működtetett ASP rendszer és annak a felhasználóival szemben támasztott informatikai biztonsági követelményeket.

Az önkormányzati ASP rendszer kapcsán kiemelten kezeljük a(z) Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata (továbbiakban Hivatal) kapcsolatos biztonsági kockázatokat. Mivel a Hivatal a saját infrastruktúráját fogja használni az ASP rendszer és alkalmazások igénybe vétele során, így a felhasználói rendszerek biztonsága nagymértékben befolyásolja a teljes önkormányzati ASP rendszer biztonságát.

A Hivatal vezetőjének célja és feladata, hogy minimalizálja a kliens (felhasználó) oldali kockázatokat.

Ennek következtében, szükséges meghatározni ASP-ben a jogosítások kérdését, és a fluktuáció miatt a felhasználók jogosításának időszakos, Hivatal szintű ellenőrzését és esetleges korrekcióját.

Általános biztonsági követelmények

- Az ASP Központtól kapott szoftveres tanúsítvány és annak jelszava nem adható át az ASP Központ által nem feljogosított személynek.
- Az önkormányzati ASP rendszerben csak a „257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről” jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bárminemű fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.
- Az önkormányzati ASP rendszerben tesztelést végezni csak az idézett Korm. rendeletben meghatározott felek jogosultak.
- Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb.
- A tenant adminisztrátor (jogosultságokat kiosztó vezető) törekszik a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál figyelembe veszi a szervezeti és működési szabályzatot, amely nem kerülhet ellentmondásba a Hivatal IBSZ-szel. Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-

kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben szerepeltetjük. Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

- A Jegyző az önkormányzati ASP-t ért biztonsági incidensek észlelését jelenti az ASP Központ (és az informatika biztonsági felelős) felé is a Kormányzati Eseménykezelő Központ mellett. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg. Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi. A Hivatal vezetőjének további kötelezettségei is vannak biztonsági incidensek kapcsán (pl. Kormányzati Eseménykezelő Központtal történő kapcsolatfelvétel), melyet a jogszabályok részleteznek.
- Ha az önkormányzati ASP-t üzemeltetői, működtetői oldalon éri biztonsági incidens, az ASP Központnak kötelessége értesítést elhelyeznie a Tájékoztatási Portál nyilvánosság elől elzárt felületén, megjelenítve a lehetséges elhárítási határidőt, illetve a keretrendszer elérhetősége esetén, a keretrendszer felületén is megjeleníteni ezeket az információkat. Ebben az esetben az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.
- A Korm. rendelet szerinti üzemeltető és működtető felek a Hatóság kérésére, utasítására is leállíthatják az önkormányzati ASP rendszert, vagy annak bizonyos elemeit (pl. kibertámadás esetén). Ebben az esetben az ASP Központ tájékoztatása addig nem fog megtörténni, amíg az incidens kiváltója, okozója, felderítése akadályokba ütközhet, azaz a Hatóság írásbeli engedélyezéséig.
- 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 hatásköre.
- 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 tároljuk.

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).

Jogszabályi hivatkozások

- Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- 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.
- 257/2016. (VIII. 31.) Korm. rendelet

Az IBSZ kiegészítés területi hatálya

A szabályzat tárgyi hatálya kiterjed a Hivatal ASP-vel kapcsolatos tevékenysége során keletkezett, kezelt, feldolgozott, tárolt adatokra és információkra, a számítástechnikai eszközökre, dokumentációikra, és az azokat körülvevő környezetre, valamint a szoftverekre, adatbázisokra, a kapcsolódó dokumentációkra és az adatbiztonsági nyilvántartásokra.

A szabályzat személyi hatálya kiterjed a Hivatal ASP rendszerrel jogosultan kapcsolatba kerülő köztisztviselőire, ügykezelőire, munkavállalóira, illetve egyéb munkavégzésre irányuló, egyéb jogviszonyban álló személyekre, továbbá a választott képviselőkre és a Hivatallal szerződéses kapcsolatban álló vállalkozóira és azok alkalmazottaira. E dokumentum a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat mellékletét képezi.

Az ASP rendszerek fizikai működésének területei:

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata

Székhely: Tolna megye 7150 Bonyhád, Széchenyi tér 12.

Védelmi intézkedések

A védelmi intézkedések megvalósulásának jelentős részét az ASP Központ biztosítja. Tekintettel azonban arra, hogy az adatkezelés a Hivatal helyszínein, a Hivatal munkavállalói és szerződött partnerei által is megvalósul, így biztonsági elvárások egy része a Hivatal hatáskörébe tartozik.

Az informatikai rendszerek ASP általi besorolása a Hivatal Informatikabiztonsági szabályzatában lett dokumentálva. Jelen szabályzat csak az ASP 2-es szintnél magasabb (a MÁK által meghatározott) védelmi kötelezettségeket, elvárásokat taglalja. A 2-es szintnek való megfelelést a Hivatal hatályos Informatikabiztonsági szabályzata írja le.

Adminisztratív védelmi intézkedések

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.

Feladatok az IT biztonsági feltételek megteremtésére, mind a 2-es biztonsági szint mind az ASP működtetéséhez elvárt szinteknek való megfelelésben.

- Önkormányzati biztonsági szintjének meghatározása.
- A meghatározott biztonsági szinthez kapcsolódó védelmi intézkedések biztosítása.
- Információbiztonsági szabályozások kialakítása, szükség szerinti módosítása, jóváhagyása, kihirdetése.
- Biztonsági auditra való felkészülés.

Fontos, hogy:

- egy az ASP-vel kapcsolatos audit tevékenység csak a Hatóság írásbeli engedélyével végezhető el. Erről az önkormányzatnak tájékoztatja a Magyar Államkincstárt.
- az ASP rendszeren külsős Fél, vagy szervezet nem végezhet sérülékenységi vizsgálatot a Hatóság írásbeli engedélye nélkül. Ezen vizsgálati tényről az önkormányzat tájékoztatja a Magyar Államkincstárt.

Munkaállomásra vonatkozó biztonsági elvárások

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

- A folyamatot változáskövetési eljárásrendbe rögzítjük.
- A munkaállomásokon telepítve van vírusvédelmi program, a legfrissebb vírus definíciós adatállománnyal. A végpontvédelem tartalmazza e-mail (csatolmány) védelmet is.
- A munkaállomáson megoldott a böngésző megfelelő biztonsági beállítása.
- A tervszerű beavatkozásokhoz karbantartási időablak jelölünk ki.
- A munkaállomások programfrissítése, különös tekintettel a legfrissebben kiadott security patch komponensekre felügyelt.
- A telepítő programok, a licenz azonosítók zárható helyen vannak tárolva.

A munkaállomások elhelyezésénél gondot fordítunk, hogy:

- 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 megoldott legyen,
- munkaidő végén a munkaállomások kikapcsolása történjen meg.

Az ASP központhoz csatlakoztatott infrastruktúra elemeknél megoldjuk a:

- a naplóinformációk védelmét,
- hiba esetén a naplóbejegyzések elemzését,
- a rendszer hozzáférés ellenőrzését.

A vírusvédelmi eljárások követelményei

- Meghatározzuk a vírusfertőzés megelőzésére vonatkozó szabályokat. (pl. működő vírusvédelmi rendszer nélkül munkaállomást, laptopot, számítógépes hálózatot nem szabad üzemeltetni. Továbbá a vírusvédelmi program vírus definíciós állományait a legfrissebb állapotban tartja.)
- A teendőket rögzítjük egy vírusfertőzés esetén.
- Vírustámadás esetén szükség szerint a vírusriadót elrendeljük.
- Sérülés, vírusfertőzés után az elvárt helyreállítási eljárások meghatározzuk.

Hálózat védelme

Az informatikai biztonságra és hálózati elérésre vonatkozó minimális és ajánlott feltételek megfogalmazása során az internet eléréshez és a hálózat kiépítéséhez, bővítéséhez szükséges eszközöket meghatároztuk (pl. router, switch, tűzfal.)

A rendszer üzemeltetésével kapcsolatos elvárások:

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) megváltoztatjuk. Az azonosítók zárt borítékban, és biztonságosan zárható helyen tároljuk. Csak előre kijelölt, privilegizált felhasználóknak engedélyezzük bejelentkezni a kérdéses eszközökbe.
- A hálózati végpontokat védjük. A lehetőségek figyelembevételével pl. port security, esetleg 802.1x szabványnak megfelelően.
- Az eszközök hálózatba történő illesztéséről dokumentáció készül.

- Az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történik.
- A menedzselhető eszközök legfrissebb konfigurációja elmentve és zárható helyen tároljuk.

Informatikai határvédelem, tűzfal

- A szervezet internethez való csatlakoztatása csak a központi tűzfalon keresztül történhet meg.
- A tűzfal szabályokat dokumentáljuk és azok zárható helyen, tároljuk.

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

Mobil eszközök használata

Az informatikai biztonság megfelelő megteremtés és szinten tartása miatt külön gondoskodunk a mobil eszközök használatának a szabályozásáról. Ehhez a betartandó szempontok a következők:

- A mobil eszközök használatát minden esetben előzetes jegyzői engedélyezés előzni meg.
- A mobil eszközök (pl. notebook) használatára a munkaállomásokra vonatkozó szabályok is érvényesek.
- Kidolgozzuk a mobil informatikai eszközök igénylésének, kiadásának, visszavételének, nyilvántartásának üzemeltetésének a folyamatait.
- Továbbá azokat a szabályokat, amelyek az eszközök hivatalon kívüli kivitelére, az eszközök javítására, esetleges elvesztésére, vagy a selejtezésére vonatkoznak.

1. Szervezeti szintű alapfeladatok

Az alapfeladatokat a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

2. Kockázatelemzés

Az alapfeladatokat a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

3. Rendszer és szolgáltatás beszerzés

Az alapfeladatokat a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

3.1. Erőforrás igény felmérés

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésben működtetett elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházások tervezése részeként;
- elkülönítetten kezeli az ASP-vel kapcsolatban saját működtetésű az elektronikus információs rendszerek biztonságát leíró dokumentumokat a beruházás tervezési dokumentációjában.

3.2. Beszerzések

A Jegyző az ASP-vel kapcsolatban saját működtetésű, az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

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

3.3. A védelem szempontjainak érvényesítése a beszerzés során

- A Jegyző védi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.
- A Jegyző ugyancsak szerződéses követelményként határozza meg az ASP-vel kapcsolatban saját működtetésű rendszerrel kapcsolatban a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

4. Üzletmenet (ügymenet) folytonosság tervezése

A Hivatal az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerek rendelkezésre állásának, valamint az EIR-ekben tárolt, illetve kezelt adatok sértetlenségének és rendelkezésre állásának megőrzése érdekében a munkavégzéshez szükséges informatikai erőforrások kiesésére vonatkozóan tervet készít, amely tartalmazza az érintett EIR-eket, az alapfeladatokat és funkciókat, a problémakezeléshez szükséges azonnali intézkedéseket, valamint a helyreállítási idő függvényében szükséges alternatív (tartalék) intézkedéseket, a

helyreállításához szükséges feladatokat és az azokhoz kapcsolódó prioritásokat, az intézkedések végrehajtásáért felelős szerepköröket feladataikat.

A Hivatal az alábbi, megelőző védelmi intézkedéseket teszi:

- megvédi a mentett információk bizalmosságát, sértetlenségét és rendelkezésre állását; ennek érdekében a mentési adathordozók tárolására elsődleges és szükség szerint másodlagos tárolási helyszínt jelöl ki, továbbá kialakítja a mentési adathordozók biztonságos tárolásának feltételeit (pl.: zárható lemezszekrény vagy páncélszekrény, elektronikus védelemmel ellátott helyiség, stb.);
- gondoskodik az informatikai eszközök rendszeres karbantartásáról, szükség szerinti javításáról;
- a kieső informatikai erőforrások (pl.: hardvereszközök) pótlásáról szükség esetén rendkívüli beszerzéssel gondoskodik;

4.1. Kritikus rendszerelemek meghatározása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekben meghatározza az elektronikus információs rendszerek alapfunkcióit támogató kritikus rendszerelemeket az üzletmenet folytonossági tervben. A tervvel kapcsolatos részleteket a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

4.2. A folyamatos működésre felkészítő képzés

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerek folyamatos működésére, felkészítő képzést tartat az Informatikabiztonsági felelős révén a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő meghatározott (az Informatikabiztonsági vezető ajánlása, de legkésőbb az éves oktatás során) időn belül;
- legalább évente egyszer, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik. Az oktatásról szóló jegyzőkönyvet, a 6.4 pont szerinti dokumentált formában megőrzi.

4.3. Üzletmenet folytonosság elérhetőség

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszer biztonsági tárolási helyszínéhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére – a Jegyző, vészhelyzeti eljárásokat dolgoz ki az üzletmenet folytonossági tervben.

4.4. Infokommunikációs szolgáltatások

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereit (a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével) amennyiben jogszabályi kötelezettsége van a saját működtetésű rendszerének folyamatos fenntartására, tartalék infokommunikációs szolgáltatásokkal létesíti és üzemelteti. Erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újratekésítését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

4.5 Szolgáltatás-prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, akkor a Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekkel kapcsolatos üzemeltetőktől megköveteli, hogy az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

5. Emberi tényezőket figyelembe vevő - személy - biztonság

Humán erőforrás az ASP-ben

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

Alkalmasság vizsgálattal kapcsolatos elvárások:

- Az önkormányzati hivatal humánpolitikai szervezet vezetőjének a felelőssége, hogy foglalkoztatás előtt a betöltendő ASP rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelési vizsgálatot végezzen el a foglalkoztatni kívánt munkatárs vonatkozásában.
- A kockázattal arányos mértékben mérlegeljük a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképeség stb.).
- Meggyőződünk arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.
- Az informatikai biztonsági szakterület vezetőjének felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.
- A humánpolitikai szakterület vezetőjének a felelőssége, hogy a foglalkoztatás alkalmával az önkormányzati hivatal munkaköri leírásban rögzítse a kockázatokkal arányosan a titoktartás követelményeit (ASP titoktartási nyilatkozat) és a foglalkoztatás egyéb kikötéseit.

- Az önkormányzati hivatal jogi szakterület vezetőjének felelőssége, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

5.1. Munkakörök, feladatok biztonsági szempontú besorolása

A Jegyző:

- minden az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerrel kapcsolatos és érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot, biztonsági szempontból besorol. A besorolás alapja kétszintű: Jogosultságot adó (tenant adminisztrátor) és végrehajtó (user);
- szükség szerint felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat (ha vannak);
- rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

5.2. A személyek ellenőrzése

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy az (5.1. pont) pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e;
- az (5.1. pont) szerinti munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében szükség szerint kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést (ha szükséges);
- folyamatosan ellenőrzi (az évenkénti felülvizsgálatok alkalmával) e pont szerinti feltételek fennállását.

5.3. Az áthelyezések, átirányítások és kirendelések kezelése

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereknél szükség esetén elvégzi az 5.2. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást;
- logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekhez;
- szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését;
- a jogviszony változásáról szóban és szükség szerint írásban (pl.: e-mail) értesíti az ASP rendszereket használó szerepköröket betöltő, feladatokat ellátó személyeket.

5.4. A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
- szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg a Jegyző és a vonatkozó rendeletek által meghatározott személybiztonsági követelményeknek;
- a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;
- előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön írásos (pl. e-mail) értesítést a Jegyzőnek;
- folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

5.5. Belső egyeztetés

A Jegyző a rendszeres Hivatali és Hivatalok közti kommunikációban egyezteti az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszert biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

6. Tudatosság és képzés

A Hivatal minden, munkaköri feladatai ellátása során az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél felhasználására kötelezett munkavállalója számára biztosítja feladatainak és szerepkörének megfelelő mértékben az adott EIR felhasználására, annak biztonsági követelményeire vonatkozóan rendelkezésre álló információkat, dokumentációkat, továbbá az ezzel kapcsolatban esetlegesen elérhető (pl.: központi üzemeltető által biztosított) képzésen történő részvételt.

A fentiek a Hivatal által használt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyekre és szervezetekre is vonatkozik, de ezen képzések nem a Hivatal feladata. Azt előírja a fenti személyeknek, szervezeteknek, oly módon, hogy igazolják annak teljesítését.

Az egyéb információbiztonsági tárgyú képzéseken, biztonság tudatosító programokon, oktatásokon történő részvétel igazolása az adott képzés, oktatás jellegétől és lebonyolítási módjától függően történhet a képzést, oktatást szervező szervezet – amennyiben az nem a Hivatal – által kiadott igazolás, illetve jelenléti ív formájában.

6.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel.

A Jegyző az IB szakmai kapcsolattartását az IB felelősön keresztül valósítja meg.

6.2. Belső fenyegetés

A Jegyző a biztonság tudatosítási képzések keretében, végzeteti az érintett személyeknek a belső fenyegetések felismerésére való felkészítését, hogy tudatosítsa jelentési kötelezettségüket. A képzésben és tudatosításban hangsúlyt fektetünk arra, hogy a hibákat, incidenseket ne titkolják el, hanem jelentsék a Jegyzőnek.

6.3. Szerepkör, vagy feladat alapú biztonsági képzés

A Jegyző szerepkör, vagy feladat alapú biztonsági képzést nyújt az Informatikabiztonsági felelős által az egyes szerepkörök szerinti, felelős személyeknek:

- az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi és évenkénti rendszerességgel.

6.4. A biztonsági képzésre vonatkozó dokumentációk

A Jegyző:

- dokumentálja a biztonság tudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;
- a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi. A dokumentumot az iratkezelési szabályzat előírásai szerint őrizzük meg és tároljuk.

Fizikai védelmi intézkedések

7. Fizikai védelmi eljárásrend

Fizikai biztonság megteremtése ASP-ben

A fizikai biztonság meghatározásánál az ASP-t futtató objektum tekintetében, az önkormányzati hivatal biztonsági zónákat jelölni ki, melyet minden esetben az önkormányzati hivatali szervezete határoz meg, saját eljárásrendjében, az alábbiak figyelembevételével:

- Az épület földrajzi elhelyezkedését. Lehetőleg a bejutás ellenőrzött legyen.
- Az épület építészeti, épületgépészeti adottságait figyelembe vesszük.
- Ügyfélforgalom mértékét,
- az ASP felhasználóknak nyújtott szolgáltatásokat és az
- információk osztályozása, minősítését figyelembe vesszük.

Őrzés, védelem szempontjai

- A törekszünk az élő erős őrzés megvalósítására. Ha ez megvalósul, akkor szabályzatban rögzítjük az őrszolgálat működési rendjét, az incidenskezelés folyamatát.
- Az önkormányzati hivatalok ASP-t is futtató helységeibe a bejutás ellenőrzötten történik az oda beosztottakon és ügyintézés miatt jelenlévőkön kívül (pl. vendégek, karbantartók stb.) ellenőrzésről nyilvántartást vezetünk.
- Hivatalunk a lehetőségeihez képest kialakít az objektum védelme érdekében behatolás védelmi, tűzjelző és szükség szerint video-megfigyelő rendszert. A biztonsági rendszerek adatai archiváljuk, és akár több hónapra visszamenőleg megőrizve a hazai jogszabályokat figyelembe véve.
- Földszinti ablakokon lehetőség szerint vasrácsokkal védekezünk az illetéktelen behatolástól. Az informatikai biztonsági felelős rendszeresen (évente) ellenőrzést hajt végre, az eredményt jegyzőkönyvbe rögzíti, mely része, kiegészítése a cselekvési tervnek. A jegyzőkönyvet az ASP Szolgáltatási szerződésben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre adja át.

7.1. Hozzáférés az adatátviteli eszközökhöz és csatornákhöz

A Jegyző engedélyhez köti és ellenőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerei adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

7.2. A kimeneti eszközök hozzáférés ellenőrzése

A Jegyző jogosultsághoz köti és ellenőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereihez, kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá. A jogosultság történhet szóban, szerződés és munkaköri feladat keretében.

7.3. A fizikai hozzáférések felügyelete

A Jegyző jogosultsághoz köti és ellenőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és szükség esetén reagáljon arra.

7.4. Behatolás riasztás, felügyeleti berendezések

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél (ha azt naplózást biztosító védelmi rendszer biztosítja) rendszeresen átvizsgáltatja a fizikai hozzáférésekről készült naplókat.

7.5. A látogatók ellenőrzése

A Jegyző az érvényes tv.-ben meghatározott ideig megőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél helyt adó létesítményekbe történt látogatói belépésekről szóló információkat. Az ilyen helyiségekbe való belépés dokumentálását, (Hivatali terület) amennyiben nincs elektronikus védelmi rendszer, akkor papíralapon dokumentáljuk és őrizzük meg.

7.6. Áramellátó berendezések és kábelezés

A Jegyző a szükséges mértékben és optimális módon védi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereit árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben (kábelcsatornák, rejtett kábelezés). Az erőforrásokat koncentráltan tartalmazó helyiségekben a hőmérsékletnek és a páratartalomnak az erőforrások biztonságos működéséhez szükséges szinten tartása és folyamatos figyelemmel kísérése, ellenőrzése céljából erre alkalmas légkondicionáló berendezést üzemeltet.

7.7. Tűzvédelem

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerei számára amennyiben azt arra alkalmas, elkülönített helységben működteti, független áramellátással támogatott érzékelő, az informatikai eszközökhöz megfelelő és a vonatkozó rendeleteknek megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

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

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél megköveteli, hogy az elektronikus információs rendszer optimális és célszerű kialakítással védjék a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek legyenek.

7.9. Be- és kiszállítás

A Jegyző mindig egyedileg engedélyezi, vagy tiltja, továbbá figyelteti és ellenőrzi a létesítménybe bevitt, onnan kivitt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszer elemeket, és nyilvántartást vezet ezekről. A be- és kiszállítás felügyeletét, figyelemmel kísérését a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személy felügyeletével megbízott munkatárs esetében is

engedélyhez köti, szakmai ellenőrzésében szükség szerint közreműködik az IT üzemeltető, rendszergazda.

7.10. Az elektronikus információs rendszer elemeinek elhelyezése

A Jegyző úgy helyezi, vagy helyezetteti el az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

7.11. Karbantartók

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemei karbantartását kizárólag a Hivatallal e feladat ellátására vonatkozóan szerződéses jogviszonyban álló szervezetek, illetve személyek az IBSz és mellékleteiben meghatározottak szerint, s minden esetben csak felügyelet mellett végezhetik. A jegyző továbbá:

- fenntart egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- felhatalmazást ad a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

7.12. Időben történő javítás

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeihez, karbantartási támogatást biztosít, szerződést köt az időben történő javítások megelőző karbantartások elvégzésére.

Logikai védelmi intézkedések

8. Általános védelmi intézkedések

8.1. Az elektronikus információs rendszer kapcsolódásai

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett rendszerek esetében a kapcsolódás szabályait, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát a rendszer tulajdonosa, működtetője határozza meg és dokumentálja. Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek használatba

vétele esetén a Hivatal gondoskodik arról, hogy ugyanezen információk a rendszer dokumentációiban szerepeljenek.

A Jegyző feladata gondoskodni arról, hogy az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereivel kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladatellátásukhoz szükséges mértékben a rendelkezésre álló rendszer-, illetve felhasználói dokumentációkat megismerjék.

8.2. Belső rendszer kapcsolatok

A Jegyző általa kiadott, engedélyhez köti az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek összekapcsolását.

8.3. Külső kapcsolódásokra vonatkozó korlátozások

A Hivatal által használt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek, illetve rendszerlemeik külső elektronikus információs rendszerhez történő kapcsolódása kizárólag a Hivatal által igénybe vett vagy jóváhagyott hálózati kommunikációs csatornán (internet kapcsolat, adathálózat) keresztül a Jegyző jóváhagyásával engedélyezett.

A végrehajtható programok, script-ek (pl.: Java Applet, JavaScript, VB Script, CGI, stb.) letöltését, futtatásának lehetőségét, valamint web és alkalmazásba csomagolt ActiveX objektumok működését letiltjuk az internet böngésző programokban, továbbá gondoskodunk arról, hogy a böngésző alkalmazás biztonsági frissítése rendszeresen megtörténjen.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett rendszerek esetében a kapcsolódás biztonsági követelményeit – fentieknél esetenként szigorúbb korlátozását, illetve az attól való eltérést – a rendszer működtetője határozza meg, a Hivatal gondoskodik annak alkalmazásáról, szabályok betartásáról.

9. Tervezés

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek tervezéssel kapcsolatos vonatkozó részleteket a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

10. Konfigurációkezelés

10.1. Legszűkebb funkcionalitás

A Hivatal az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek a felügyeletét és konfigurációs beállításait a legszűkebb funkcionalitás elvének megfelelően, a nem szükséges funkciók, portok, protokollok, szolgáltatások korlátozásával, illetve tiltásával határozza meg és dokumentálja. A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott EIR használatához szükséges és elégséges konfigurációs beállításokat. Továbbá meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

10.2. Duplikálás elleni védelem

A Jegyző ellenőrzi, hogy az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

11. Karbantartás

11.1. Adathordozó ellenőrzés

A Jegyző ellenőrizteti a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

11.2. Távoli karbantartás

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

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

12. Adathordozók védelme

12.1. Adathordozók tárolása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- fizikailag egyedileg azonosítja, ellenőrzi és biztonságosan tárolja az adathordozókat az arra engedélyezett vagy kijelölt (elzárt) helyen;
- védi (és ezt a munkatársaitól is megköveteli) az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

A hivatali munkavégzéshez a Hivatal által biztosított, beépített adathordozót tartalmazó mobil eszközök (pl.: laptop, tablet, okostelefon) és mobil adattároló eszközök (pl.: memóriakártya, külső háttértároló eszköz vagy merevlemez, optikai adathordozó lemez, stb.) fizikai védelméről és biztonságos tárolásáról és kezeléséről a használatára jogosult személy, munkavállaló köteles gondoskodni. Használaton kívül az eszközt, adattárolót elzárjuk, illetve illetéktelenek számára hozzáférhető helyen folyamatos felügyelet nélkül, őrizetlenül hagyni (pl.: közterületen parkoló zárt gépjárműben is) nem szabad!

12.2. Adathordozók szállítása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél :

- az IBSZ-ben leírt biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;
- biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;
- feljegyzésben dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;
- korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

12.3. Kriptográfiai védelem

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél megköveteli, hogy kriptográfiai mechanizmusokat alkalmazzanak a digitális adathordozókon tárolt információk bizalmosságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás, használat folyamán (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.). A kriptográfiai védelem megvalósítása az eszköz e célt szolgáló funkciójának használatával történhet (pl.: BitLocker meghajtótitkosítás, VPN), melyek esetében a technológia (pl.: OpenVPN, SSTP, stb.), illetve az általa alkalmazott rejtjelezési algoritmus (pl.: AES) megfelelősége nemzetközileg elismert információbiztonsági szabvány alapján (pl.: CC, FIPS) igazolt.

12.4. Ismeretlen tulajdonos

A Jegyző megtiltja az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

13. Azonosítás és hitelesítés

ASP rendszerbe történő belépés, autentikáció

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 autentikáció során a következő szabályokra megkülönböztetett módon figyelünk:

- Minden ASP rendszert használó munkatársnak rendelkezik 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 autentikációs folyamat céljából másnak átadni tilos.
- Az hivatal vezetője a Jegyző gondoskodik arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen.

13.1. Jelszó (tudás) alapú hitelesítés

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvényrel a jelszóból képzett hasító érték tárolást), és nem továbbítja;

A jelszavas hitelesítést alkalmazó rendszerelemeken kötelező a jelszavas védelem beállítása és alkalmazása.

A felhasználói jelszavakra vonatkozó a mindig a technikailag elvárt, de minimálisan alkalmazandó általános jelszó követelmények:

- a jelszó minimális hossza (legrövidebb jelszó): 8 karakter;
- a jelszó bonyolultsága (komplexitás): tartalmaz legalább egy kis- és nagybetűs, speciális karaktert, valamint számjegyet;
- előző jelszavak megőrzése: legutolsó 5 jelszó tárolása;
- a jelszavak minimális és maximális élettartama: 0 és 90 nap.

A meghatározott jelszóképzési szabálytól eltérni a jelszó hosszát, bonyolultságát illetően a magasabb védelmi szintet jelentő irányba, felfelé lehet (pl.: „jelszó helyett jelmondat”-elv alkalmazásával).

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által meghatározott jelszóképzési szabályokat alkalmazza.

A felhasználói jelszavakat tilos papír alapon, felírva tárolni! Kivételt képeznek ez alól a privilegizált hozzáférésekhez tartozó azonosítók és jelszavaik, melyeket rendelkezésre állásuk folyamatos biztosítása érdekében a Jegyző gondoskodik azok biztonságos megőrzéséről és kezeléséről (lezárt borítékban, páncélszekrényben).

A felhasználói azonosítók és jelszavak elektronikus tárolása, nyilvántartása kizárólag önálló és biztonságos hitelesítési megoldással rendelkező vagy egyéb kriptográfiai védelemmel ellátott módon, offline tárolással engedélyezett; nyílt formában vagy mobil infokommunikációs eszközön valamint online jelszótároló rendszerben tilos!

Az internetkapcsolaton keresztül elérhető EIR-ek, illetve rendszerelemeik esetében az internet böngészőprogramok beépített kényelmi funkciójának, a bejelentkezési adatok tárolásának (pl.: automatikus kiegészítés, felhasználói jelszavak megjegyzése) a használata tilos, a funkciót kikapcsoljuk!

13.2. Birtoklás alapú hitelesítés

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

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

Ha a Hivatal hatáskörébe tartozik, akkor azt minden esetben átadás-átvételi bizonylattal dokumentálja. Az átadás-átvétel dokumentumainak megőrzéséről a Hivatal a hatályos iratkezelési szabályainak megfelelően gondoskodik.

A jegyző a birtoklásalapú hitelesítésre szolgáló eszközök használati idejét, továbbá ismételt felhasználhatóságának feltételeit az érintett EIR igénybevételére vonatkozó szabályok, valamint a kibocsátó, illetve a gyártó ajánlásainak megfelelően alakítja ki, illetve alkalmazza.

13.3. Személyes vagy megbízható harmadik fél általi regisztráció

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

14. Hozzáférés ellenőrzése

14.1. A felelőségek szétválasztása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- szétválasztja az egyéni felelőségeket;
- dokumentálja az egyéni felelőségek szétválasztását;
- meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelőségek szétválasztása érdekében.

14.2. Legkisebb jogosultság elve

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

14.3. Jogosult hozzáférés a biztonsági funkciókhoz

A Jegyző hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

14.4. Nem privilegizált hozzáférés a biztonsági funkciókhoz

A Jegyző kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

14.5. Privilegizált fiókok

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

14.6. A munkaszakasz zárolása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- kötelezi a felhasználókat, hogy 5 perc inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;
- megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

14.7. Képernyőtakarás

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - eltakarjuk.

14.8. A munkaszakasz lezárása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél automatikusan lezárja a munkaszakaszt a meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

14.9. Vezeték nélküli hozzáférés

A Hivatal épületeiben vezeték nélküli hálózatához hozzáférést a Jegyző engedélyével lehet csak létesíteni, illetve igénybe venni. Kivételt képez ez alól – amennyiben az adott telephelyen elérhető – a Hivatal által biztosított, a Hivatal hálózatáról leválasztott, szeparált nyilvános hálózati hozzáférés (pl.: „vendég” wifi), amelyhez a Hivatal munkatársai is csatlakoztathatják saját mobil eszközeiket.

Hivatali munkavégzés céljára biztosított vezeték nélküli hálózat hozzáférés védelemmel (minimum jelszavas védelemmel) ellátottan és a csatlakoztatható eszközök – például fizikai hálózati címének (MAC address filter) – szűrésével létesíthető.

A Jegyző:

- az engedélyezési és jogosultsági szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
- engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

14.10. Mobil eszközök hozzáférés ellenőrzése

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- az engedélyezési és jogosultsági szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;
- engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

14.11. Titkosítás

A Jegyző teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk

bizalmosságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

14.12. Korlátozott használat

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

- előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy
- jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

14.13. Hordozható adattároló eszközök

A Jegyző egyedileg korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a jogosultsággal rendelkező személyek számára.

14.14. Információ megosztás

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- elősegíti az információ-megosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információ-megosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;
- automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információ-megosztási vagy együttműködési döntések meghozatalában.

15. Rendszer és információ sértetlenség

15.1. Automatikus frissítés

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

15.2. Biztonsági riasztások és tájékoztatások

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- folyamatosan figyeli, illetve az informatikai biztonsági felelősön keresztül figyelteti a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri, illetve az informatikai biztonsági felelősön keresztül figyelteti a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
- szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;
- a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
- kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart illetve az informatikai biztonsági felelősön keresztül tartat az érintett, külön jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz, vagy intézkedik annak tételére a megbízott személyekkel, szervezetekkel.

15.3. Bemeneti információ ellenőrzés

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél ellenőrzi a meghatározott információ belépési pontok érvényességét.

Jelen kiegészítés a Hivatali IBSZ-szel együtt értelmezendő, a továbbiakban egy dokumentumként kezelendő. Hatályba lépésének napja megegyezik a Hivatali IBSZ hatálybalépésének idejével.

A Hivatal kliens oldali biztonsága megteremtésének táblázatos összefoglalója

Az ASP kapcsán kiemelten kezeljük a Hivatallal kapcsolatos biztonsági kockázatokat. A Hivatal a saját infrastruktúráját fogja használni az alkalmazások igénybevétele során, így a kliens rendszerek biztonsága nagymértékben befolyásolja a teljes ASP rendszer biztonságát.

A lehetséges fenyegetettségek, sebezhetőségek, valamint ezek megelőzésére alkalmazható intézkedések a Hivatalunkban az alábbiak:

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.


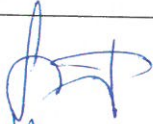

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	Az Internet böngészőkben meglévő biztonsági „lyukak” megszüntetésére szolgáló javító programok letöltésének elmulasztása. A biztonsági „lyukak” kihasználásával elérhető a végponti felhasználó érzékeny adatai (jelszó, az állomás konfigurációja, fájl 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.
	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.

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

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során kötelesek vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Filóné Ferencz Ibolya polgármester		2021. X. 01.
Filczinger Ágnes jegyző		2021. X. 01.
Dr. Márton Antal aljegyző		2021. X. 01.


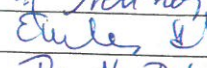
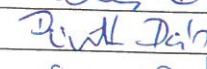
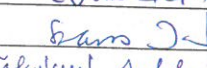
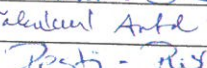
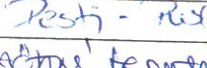

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Visnyei Gabriella	<i>Visnyei Gabriella</i>	2021. 10. 01.
Budainé Szomolai Csilla	<i>Budai Csilla</i>	2021. 10. 01.
Molnár Sándorné	<i>Molnár Sándorné</i>	2021. 10. 01.
Palkó Helga	<i>Palkó Helga</i>	2021. 10. 01.
Pausch Mihályné	<i>Pausch Mihályné</i>	2021. 10. 01.
Jakabné Antal Mónika	<i>Jakabné Antal Mónika</i>	2021. 10. 01.
Joó Bella Szabina	<i>Joó Bella Szabina</i>	2021. 10. 01.
Jakabné Juhász Éva	<i>Jakabné Juhász Éva</i>	2021. 10. 01.
Surján Veronika	<i>Surján Veronika</i>	2021. 10. 01.
Borbáth Krisztina	<i>Borbáth Krisztina</i>	2021. 10. 01.

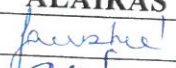
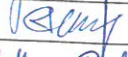
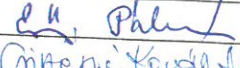
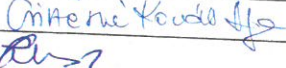
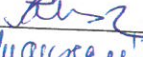
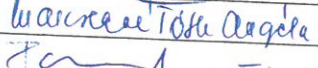

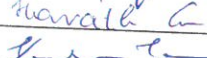
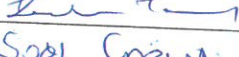
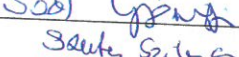
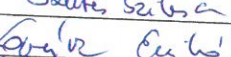
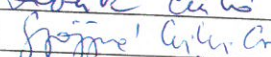
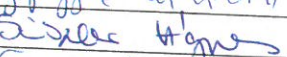
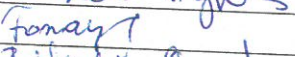
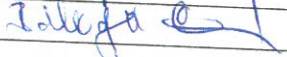

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Dr. Brandt Huba		2021. 10. 01.
Énekes Andrea		2021. 10. 01.
Pintérmé Dávid Edit		2021. 10. 01.
Szarvas Irén		2021. 10. 01.
Takácsné Antal Tünde		2021. 10. 01.
Pesti-Pusch Adrienn		2021. 10. 01.
Szötsné Szentes Rita		2021. 10. 01.

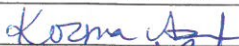







Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Fauszt Józsefné		2021. 10. 01.
Palkó Roland		2021. 10. 01.
Erős Pálné		2021. 10. 01.
Csiszerné Kovács Ibolya		2021. 10. 01.
Kiszler-Rausch Etelka		2021. 10. 01.
Dr. Marcsekne Tóth Angéla		2021. 10. 01.
Palkovics Judit		2021. 10. 01.
Horváth Csilla		2021. 10. 01.
Kerekes Kornélia		2021. 10. 01.
Soós Gyöngyi		2021. 10. 01.
Szentes Szilvia		2021. 10. 01.
Lovász Enikő		2021. 10. 01.
Györgyné Csiki Éva		2021. 10. 01.
Sizler Ágnes		2021. 10. 01.
Forrayné Hajdú Judit		2021. 10. 01.
Balogh Erzsébet		2021. 10. 01.

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Kozma Anikó		2021. X. 01.
Havasi Béla		2021. 10. 01.
László Zoltán		2021. X. 01.
Makovics István		2021. 10. 01.
Kaiser Mária		2021. X. 01.
Simonics Ottó		2021. 10. 01.
Magyari Balázs		2021. 10. 01.
Simon Zsolt		2021. 10. 01.

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Kelemenné Dudás Bettina	Kelemenné Dudás Bettina	2021. 10. 01.
Farkasné Szentpál Melinda	Farkasné Szentpál Melinda	2021. 10. 01.
Váczi Mária	Váczi Mária	2021. 10. 01.


Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Horváth Jánosné	Horváth Jánosné	2022.12.06
Novotni Józsefné	Novotni Józsefné	2022.12.06.
Simondi Zoltánné	Simondi Zoltánné	2022.12.06.

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Höfler-Varga Mónika		2021. X. 01

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Nagy Nikoletta	<i>Nagy Nikoletta</i>	2023. 12. 07.

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Bálint Lászlóné	Bálint Lászlóné	2021. Október 1

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Ludvig Gréta	<i>Lu</i>	2021. 10. 01.

Megismerési nyilatkozat

Aláírással igazolom, hogy a Bonyhádi Közös Önkormányzati Hivatal Polgármesterének és Jegyzőjének 3/2021. (X.01.) utasításában foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	ALÁÍRÁS	DÁTUM
Kasler Lászlóné	<i>Kasler Lászlóné</i>	2022. 10. 01.