FÜZESYARMAT VÁROS ÖNKORMÁNYZATA

INFORMATIKAI BIZTONSÁI SZABÁLYZAT

Kelt: 2019. február 11.

Verzió: V 1.0

Tartalomjegyzék

1.1 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) Füzesgyarmat 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

Az Informatikai Biztonsági Szabályzat összhangban van a Hivatal minőségirányítási rendszerét leíró dokumentumokkal.

1.1.1 A dokumentum célja

A szabályzat célja, hogy az adatbiztonság érvényesítése, az egyes szoftverekhez való hozzáférési jogok meghatározása, az ellenőrzési mechanizmusok meghatározása, a felelősségi viszonyok tisztázása, az egyes adatkezelő műveletek részletezése az adatvédelmi és az iratkezelési szabályzattal, illetve a vonatkozó jogszabályi előírásokkal összhangban történjen.

1.1.2 A dokumentum hatálya

A szabályzat tárgyi hatálya kiterjed a Hivatal 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 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.

1.1.3 Alapfogalmak

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.1.4 Szerepkörök

A Polgármesteri hivatal a részletes hivatali szerepköröket a Szervezeti és Működési Szabályzatban rögzítette.

Polgármesteri hivatal (képviselő testület, jegyző, polgármester): az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, stratégiát, politikát határoz meg, felügyeli ezek megvalósulását, forrást biztosít a megvalósításokhoz.

Informatikai referens: az informatikabiztonsággal kapcsolatban szervezi, és szakmai kompetenciájának megfelelően végrehajtja a Polgármesteri hivatal által meghatározott politikát, célokat, stratégiát. Kapcsolatot tart és felügyeli a feladatok végrehajtásával megbízott személyt, vagy személyeket.

Informatikabiztonsági felelős- az a szakember, aki szakmailag kompetens és ellátja az informatikabiztonsággal kapcsolatos törvényi feladatokat.

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

1.1.5 Tevékenységek

A polgármesteri hivatal a tv.-ben meghatározott alaptevékenységét a Szervezeti és Működési Szabályzatban rögzítette.

1.1.6 Hivatalrendszer belső együttműködése

A polgármesteri hivatal a belső együttműködését a Szervezeti és Működési Szabályzatban rögzítette.

2.1 Besorolási Nyilatkozat

Füzesgyarmat Város Önkormányzata nyilatkozatban rögzíti, hogy a 2014.06 hó időszakban külsős szakember által egy kockázatértékelés során végzett L_2013 tv. –nek való megfelelés vizsgálatának eredményeként a Hivatal biztonsági szintje:

2-es (azaz kettes) besorolású

Indoklás:

- A szervezet által működtetett és kockázatértékelés során vizsgált elektronikus információs rendszerek egyike sem magasabb a 2-es biztonsági osztálynál.
- Hivatalunkban az elektronikus információs rendszerek biztonságához kapcsolódó eljárások teljes kialakítására törekszünk, de ehhez belső forrásból sem megfelelő szaktudás, sem megfelelő eszközrendszer nem áll még rendelkezésünkre.
- Hivatalunkban az információs rendszerek biztonságával kapcsolatos felelősségeket és feladatokat egy, az elektronikus információs rendszer biztonságáért felelős, irányítási jogkörében korlátozott személyhez rendeltük hozzá.
- Hivatalunkban az elektronikus információs rendszerek és szolgáltatások nyilvántartása nem teljes körű.
- Hivatalunkban az adathordozók nyilvántartása, kezelése, törlése nem teljes körű.
- Hivatalunkban az elektronikus információs rendszerek biztonsági felügyelete nem automatizált.
- Hivatalalunkban az elektronikus információs rendszerek előállítanak a biztonságra vonatkozó információkat, de azokat a szervezet nem elemzi.
- A hiányosságok pótlására Hivatalunk intézkedési tervet fog készíteni, melyhez határidőket és felelős személyeket fog hozzárendelni.

Kelt: 2019. február 11.

Aláírás, PH

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

3.1 Adminisztratív Védelmi Intézkedések

Szervezeti szintű alapfeladatok

3.1.1.1 Informatikai biztonságpolitika

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonságpolitikát. Az informatikai biztonságpolitikát a Hivatal vezető testülete hagyja jóvá.

A Hivatal vezető testülete a biztonságpolitikában kiberbiztonsági célokat határoz meg, felállítja az informatikai biztonságpolitika hivatali szempontú alapelveit, bemutatja az érintett hivatal vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítására és támogatására, kifejti az érintett hivatalban alkalmazott biztonsági alapelveket és megfelelőségi követelményeket. Az informatikai biztonságpolitikát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a biztonságpolitikát újra vizsgálja, szükség szerinti módosítja.

A Hivatal a részéletes informatikai biztonságpolitikát egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonságpolitika)* kezeli.

3.1.1.2 Informatikai biztonsági stratégia

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági stratégiát. Az informatikai biztonsági stratégiát a Hivatal vezető testülete hagyja jóvá.

A Hivatal vezető testülete az informatikai biztonsági stratégiában a rövid, közép és hosszú távú célokat határozza meg. Az informatikai biztonsági stratégia illeszkedik az érintett hivatal más stratégiáihoz (így különösen az informatikai biztonságpolitikához, a költségvetési és humánerőforrás tervezéshez, valamint a tevékenységi kör változásához, fejlesztéshez), jövőképéhez. Az informatikai biztonsági stratégiát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági stratégiát újra vizsgálja, szükség szerinti módosítja.

A Hivatal a részéletes informatikai biztonsági stratégiát egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonsági Stratégia)* kezeli.

3.1.1.3 Informatikai biztonsági szabályzat

A Hivatal megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatát. Az informatikai biztonsági szabályzat a Hivatal, vezető testülete hagyja jóvá.

Az informatikai biztonsági szabályzatát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az informatikai biztonsági szabályzatot újra vizsgálja, szükség szerinti

módosítja. A Hivatal az „informatikai biztonsági jelentésben” rögzíti az érintett hivatal elvárt biztonsági szintjét, valamint az érintett hivatal egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

A Hivatal a részéletes informatikai biztonsági szabályzat egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonsági Szabályzat)* kezeli.

3.1.1.4 Az elektronikus információs rendszerek biztonságáért felelős személy

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

3.1.1.5 Pénzügyi erőforrások biztosítása

A Hivatal vezetése a költségvetés tervezése és a beruházások, beszerzések során az ide vonatkozó törvényben meghatározott határidőkkel tervezi az informatikai biztonsági stratégia megvalósításához szükséges forrásokat. Intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásáról. Dokumentálja e követelmény alá eső kivételeket.

3.1.1.6 Intézkedési terv és mérföldkövei

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

A Hivatal a részéletes intézkedési tervet egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Informatikai Biztonsági Stratégia)* kezeli.

3.1.1.7 Az elektronikus információs rendszerek nyilvántartása

A Hivatal az elektronikus információs rendszereiről, minden rendszerre nézve nyilvántartást vezet, azt szükség szerint aktualizálja. A nyilvántartás tartalmazza:

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

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

3.1.1.10 Kockázatkezelési stratégia

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatkezelési stratégiát. A kockázatkezelési stratégiát szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer

felülvizsgálata során (belső audit) a Hivatal felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a kockázatkezelési stratégiát újra vizsgálja, szükség szerinti módosítja.

A stratégia kiterjed:

a) a lehetséges kockázatok felmérésére;
b) a kockázatok kezelésének felelősségére;
c) a kockázatok kezelésének elvárt minőségére.

A Hivatal a részletes kockázatkezelési stratégiát és módszertant egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Kockázatkezelési Szabályzat)* kezeli.

3.1.1.11 Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat. Felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát, meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségeket, kijelöli az ezeket betöltő személyeket, integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a Hivatali szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett Hivatal hatókörébe tartozó:

a) emberi, fizikai és logikai erőforrásra,
b) eljárási és védelmi szintre és folyamatra

A Hivatal az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárást egy külön dokumentumban *(Engedélyezési és Jogosultsági Szabályzat)* kezeli.

3.1.2 Kockázatelemzés

3.1.2.1 Kockázatelemzési eljárásrend

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

A Hivatal a részletes kockázatkezelési eljárást és módszertant egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Kockázatkezelési szabályzat)* kezeli.

3.1.2.2 Biztonsági osztályba sorolás

A Hivatal jogszabályban meghatározott szempontok alapján megvizsgálja (alvállalkozó igénybevétele esetén megvizsgáltatja) elektronikus információs rendszereit, és a 3.1.1.7 pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók.

A Hivatal vezetése jóváhagyja a biztonsági osztályba sorolást, és dokumentumban *(Informatikai Biztonsági Szabályzat)* rögzíti annak eredményét.

A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten elvégzi.

3.1.2.3 Kockázatelemzés

A Hivatal végrehajtja a biztonsági kockázatelemzéseket és rögzíti azok eredményét *(a NEIH módszertani segédletben)*. A kockázatkezelési szabályzatnak megfelelően felülvizsgálja a kockázatelemzések eredményét és megismerteti a kockázatelemzés eredményét az érintettekkel.

Amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre a Hivatal.

A Hivatal gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek hozzáférhetőek, megismerhetőek. A kockázatelemzési eredményeket bizalmasan kezeli.

3.1.3 Tervezés

3.1.3.1 Biztonságtervezési eljárásrend

Biztonságtervezési szempontból a Hivatal az alábbi időszakokat definiálja az információs rendszerek életciklusának tekintetében:

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

A rendszerbiztonság tervezésekor a Hivatal az információs rendszerek valamennyi életciklusára vonatkozóan szem előtt tartja az Informatikai Biztonságpolitikában megfogalmazott célokat és követelményeket, valamint a gyártói és iparági előírásokat, ajánlásokat.

3.1.3.2 Rendszerbiztonsági terv

A Hivatal vezetése az elektronikus információs rendszereihez rendszerbiztonsági tervet készíttet, amely:

a) összhangban áll az Informatikai Biztonságpolitikával és 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.

3.1.3.2.1 Kivételek

Ha egy adott információs rendszer jelentősége nem indokolja, vagy a különböző jogi, szabályozási, vagy üzemeltetési körülmények nem teszik lehetővé, a Hivatal vezetése eltekint a rendszerbiztonsági terv megkövetelésétől.

3.1.3.3 Személyi biztonság

A Hivatal:

a) megfogalmazza és a Hivatalra 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;
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) 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;
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.

3.1.3.3.2 Viselkedési szabályok az interneten

A Hivatal:

a) tiltja és számon kéri a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
b) tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységeket (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);
c) tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a Hivataltól idegen tevékenységet.

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

3.1.4 Rendszer és szolgáltatás beszerzés

3.1.4.2 Beszerzési eljárásrend

A Hivatal vezetése megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a beszerzési eljárásrendet *(Beszerzési és karbantartási szabályzat)*, mely az érintett Hivatal elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére

vonatkozó szabályait fogalmazza meg és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő. A szabályzatot a szükséges mértékben és meghatározott gyakorisággal felülvizsgálja.

3.1.4.4 A rendszer fejlesztési életciklusa

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

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

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

3.1.4.4.2 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).

3.1.4.8 Külső elektronikus információs rendszerek szolgáltatásai

A Hivatal:

a) szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;
b) meghatározza és dokumentáltatja az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
c) külső és belső ellenőrzési eszközökkel ellenőrizteti, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

3.1.6 Emberi tényezőket figyelembe vevő – személy – biztonság

3.1.6.5 Eljárás jogviszony megszűnésekor

A Hivatal:

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

3.1.6.8 Fegyelmi intézkedések

A Hivatal fenntartja magának a jogot, hogy a jelen IBSZ-t megsértőkkel szemben eljárjon. Az eljárást a Hivatal jegyzője vagy az IT referens kezdeményezheti. A kezdeményezést a Hivatal vezetője felülvizsgálja, a szükséges intézkedéseket elrendelheti. Az IBSZ megsértése esetén az intézmény megvonhatja a hálózat, illetve a gépek használatának jogát határozott időre, vagy határozatlan időre, visszavonásig.

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

3.1.7 Tudatosság és képzés

3.1.7.1 Képzési eljárásrend

A Hivatal rendszeres képzésben részesíti az információs rendszer felhasználóit. A képzések gyakoriságát az információs rendszerek változásainak és egyéb igényeknek a figyelembevételével kell meghatározni, de évente legalább egyszer továbbképzésen kell részt vennie minden munkavállalónak. A szervezetbe újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben kell részesíteni.

A Hivatal vezetése:

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

Az IT referens:

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

3.1.7.2 Biztonságtudatossági képzés

A Hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

a) az új felhasználók kezdeti képzésének részeként;
b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
c) a Hivatal vezetése által meghatározott gyakorisággal, de minimum évente egyszer

3.2 Fizikai Védelmi Intézkedések

3.2.1 Fizikai és környezeti védelem

3.2.1.2 Fizikai védelmi eljárásrend

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

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

3.2.1.3 Fizikai belépési engedélyek

A Hivatal:

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

3.2.1.4 A fizikai belépés ellenőrzése

A Hivatal:

a) kizárólag a szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
b) naplózza a fizikai belépéseket;
c) ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
d) kíséri a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
e) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
f) nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
g) 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;
h) az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
i) a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel;
j) felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

3.3 Logikai Védelmi Intézkedések

3.3.1 Konfigurációkezelés

3.3.1.1 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.

3.3.1.2 Alapkonfiguráció

Azon információs rendszereknél, ahol indokolt és technikailag lehetséges, a Hivatal egy-egy alapkonfigurációt fejleszt ki, dokumentáltatja és karbantartatja azt, valamint leltárba foglalja a rendszer lényeges elemeit.

3.3.1.8 Elektronikus információs rendszerelem leltár

A Hivatal leltárt készít az elektronikus információs rendszer elemeiről, amit naprakészen tart annak érdekében, hogy:

a) pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
b) az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet, valamint azok licenceit tartalmazza;
c) legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

3.3.1.10 A szoftverhasználat korlátozásai

A Hivatal:

a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;
b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;
c) ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

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

3.3.1.11 A felhasználó által telepített szoftverek

A Hivatal információs rendszereire, valamint azok számítógépeire és egyéb komponenseire csak a rendszergazdák telepíthetnek szoftvereket, valamint azok rendszerszintű beállításait is csak ők (vagy az általuk megbízott külsős szakértők) jogosultak megváltoztatni.

3.3.2 Üzletmenet- (ügymenet-) folytonosság tervezése

3.3.2.1 Üzletmenet-folytonosságra vonatkozó eljárásrend

Az információk védelmének és a megfelelő rendelkezésre állásának biztosítása érdekében a Hivatal az alábbi elvárásokat fogalmazza meg az üzletmenet-folytonossági tervekkel szemben:

a) biztosítsák, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezetnél (ne sérüljön az SLA);

b) adjanak megfelelő alapot a kockázatok csökkentésére irányuló hatékony intézkedések végrehajtásához és eredményességük nyomon követéséhez;
c) határozzák meg azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a Hivatal folyamatos működése biztosítva legyen;
d) határozzák meg azokat az intézkedéseket, feladatokat, melyeket az esetleges folytonosság megszakadásra felkészülésként, illetve bekövetkezésekor a kár enyhítéseként, illetve a helyreállításért kell tenni;
e) biztosítsák, hogy az üzletmenet-folytonosság és a szolgáltatások rendelkezésre állása személyes felelősséghez köthető legyen;
f) illeszkedjenek a Hivatal közép és hosszú távú stratégiáihoz és céljaihoz;

3.3.2.2 Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

A Hivatal vezetése által az elektronikus információs rendszerekhez készíttetett rendszerbiztonsági terveknek tartalmazniuk kell az adott elektronikus rendszer (szolgáltatás) üzletmenet-folytonossági tervét is, amely:

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

A Hivatal az elektronikus információbiztonsággal kapcsolatos üzletmenet-folytonossági terveket rendszerenként külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben kezeli.

3.3.2.8 Az elektronikus információs rendszer mentései

A Hivatal a rendszerbiztonsági és üzletmenet-folytonossági elvárásokkal összhangban:

a) meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
b) meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

c) meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;
d) megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

A Hivatal az információs rendszerek mentésével kapcsolatos elvárásait (mentések gyakorisága a tolerálható adatvesztés függvényében, elvárt helyreállítási idő, megőrzési idő, offsite példányok, stb.) rendszerenként külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben kezeli.

3.3.2.9 Az elektronikus információs rendszer helyreállítása és újraindítása

A Hivatal gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

A Hivatal az elektronikus információbiztonsággal kapcsolatos helyreállítási szabályokat, valamint az elektronikus információs rendszer helyreállításának, újraindításának menetét az érintett rendszerre vonatkozó dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben kezeli.

3.3.3 Karbantartás

3.3.3.1 Rendszer karbantartási eljárásrend

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

A Hivatal az elektronikus információbiztonsággal kapcsolatos karbantartási szabályokat egy külön dokumentumban *(Beszerzési és Karbantartási Szabályzat)* kezeli.

3.3.3.2 Rendszeres karbantartás

A Hivatal által megbízott személyek vagy vállalkozók:

a) a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal követelményeinek megfelelően;
b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Hivatali létesítményből;
d) az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;
e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
f) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

A Hivatal az elektronikus információbiztonsággal kapcsolatos karbantartási szabályokat egy külön dokumentumban *(Beszerzési és Karbantartási Szabályzat)* kezeli.

3.3.4 Adathordozók védelme

3.3.4.1 Adathordozók védelmére vonatkozó eljárásrend

Az adathordózónak minősülő olyan eszközök (pl. floppy, CD, USB eszközök, külső merevlemezek, stb.) kezelésének általános irányelvei:

a) minél nagyobb mértékben járuljon hozzá az adathordozók kezeléséből eredő kockázatok csökkentéséhez;
b) tegye lehetővé valamennyi, a tevékenységet érintő adathordozók kezelésével kapcsolatos fenyegető esemény azonosítását;

3.3.4.2 Hozzáférés az adathordozókhoz

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

3.3.4.6 Adathordozók törlése

A Hivatal a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a hivatali ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt. A törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

3.3.4.7 Adathordozók használata

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

3.3.5 Azonosítás és hitelesítés

3.3.5.1 Azonosítási és hitelesítési eljárásrend

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

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

3.3.5.2 Azonosítás és hitelesítés (szervezeten belüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a Hivatal felhasználóit, a felhasználók által végzett tevékenységet.

3.3.5.4 Azonosító kezelés

A Hivatal:

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

3.3.5.5 A hitelesítésre szolgáló eszközök kezelése

A Hivatal vezetése által kijelölt személy:

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

3.3.5.6 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.

3.3.5.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A szervezet jelenleg egyik rendszeréhez sem biztosít hozzáférést külső felhasználók számára.

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

3.3.5.8.2 Hitelesítés szolgáltatók tanúsítványának elfogadása

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

3.3.6 Hozzáférés ellenőrzése

3.3.6.1 Hozzáférés ellenőrzési eljárásrend

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

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

3.3.6.2 Felhasználói fiókok kezelése

A Hivatal:

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

b) kijelöli a felhasználói fiókok fiókkezelőit;
c) kialakítja a csoport- és szerepkör tagsági feltételeket;
d) meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;
e) létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
f) ellenőrzi a felhasználói fiókok használatát;

…értesíti a fiókkezelőket, ha:

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

…feljogosít az elektronikus információs rendszerhez való hozzáférésre:

a) az érvényes hozzáférési engedély,
b) a tervezett rendszerhasználat,
c) az alapfeladatok és funkcióik alapján;

A Hivatal meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot.

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

3.3.6.3 Hozzáférés ellenőrzés érvényesítése

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

3.3.6.12 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

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

3.3.6.16 Külső elektronikus információs rendszerek használata

A Hivatal 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.

3.3.6.18 Nyilvánosan elérhető tartalom

A Hivatal:

a) kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivataltól kapcsolatos bármely információ közzétételére;
b) a kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;
c) közzététel előtt átvizsgálja a javasolt tartalmat;

d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.

3.3.7 Rendszer- és információsértetlenség

3.3.7.2 Rendszer- és információsértetlenségére vonatkozó eljárásrend

A rendszer- és információsértetlenség megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

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

3.3.7.3 Hibajavítás

A Hivatal:

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

3.3.7.4 Kártékony kódok elleni védelem

A Hivatal:

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 riassza a rendszeradminisztrátort és az érintett Hivatal által meghatározott további személy(eke)t;
c) ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

3.3.7.5 Az elektronikus információs rendszer felügyelete

A Hivatal:

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

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.

3.3.7.6 A kimeneti információ kezelése és megőrzése

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

3.3.8 Naplózás és elszámoltathatóság

3.3.8.1 Naplózási eljárásrend

A Hivatal az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként külön dokumentumban *(Rendszerbiztonsági terv)* és mellékleteiben határozza meg, az alábbi általános követelmények figyelembevételével:

3.3.8.2 Naplózható események

A Hivatal az érintett elektronikus információs rendszerre vonatkozó rendszerbiztonsági tervben:

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

3.3.8.3 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.

3.3.8.8 Időbélyegek

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a Hivatal által meghatározott időmérési pontosságnak.

3.3.8.9 A napló információk védelme

Az elektronikus információs rendszer megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

3.3.8.11 A naplóbejegyzések megőrzése

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

3.3.8.12 Naplógenerálás

Az elektronikus információs rendszer:

a) biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.8.2 pontban meghatározott, naplózható eseményekre;
b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;
c) naplóbejegyzéseket állít elő a 3.3.8.2 pont szerinti eseményekre, a 3.3.8.3 pontban meghatározott tartalommal.

3.3.9 Rendszer- és kommunikációvédelem

3.3.9.1 Rendszer- és kommunikációvédelmi eljárásrend

A rendszer- és kommunikációvédelem megvalósítása során a Hivatal az informatikai biztonságpolitikában meghatározott célok és követelmények 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:

3.3.9.6 A határok védelme

Az elektronikus információs rendszer:

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

3.3.9.10 Kriptográfiai kulcs előállítása és kezelése

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

3.3.9.11 Kriptográfiai védelem

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

3.3.9.12 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.

Kelt: 2019. február 11.

Aláírás, PH