A belügyminiszter 29/2010. (XII. 31.) BM utasítása a Belügyminisztérium Informatikai Biztonsági Szabályzatáról

A Belügyminisztérium Szervezeti és Működési Szabályzatáról szóló 7/2010. (IX. 2.) BM utasítás 84. § (1) bekezdés k) pontja alapján, az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet 38. § (3) bekezdésére tekintettel, figyelembe véve a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 8., 12., 13., 16. és 17. számú ajánlásait, továbbá a 25. számú Magyar Informatikai Biztonsági Ajánlást, a Közigazgatási Informatikai Bizottság 19. számú ajánlását, alkalmazva a COBIT és az ITIL módszereket, a Belügyminisztérium informatikai rendszereinek védelmére kiadom az alábbi utasítást:

1. A Belügyminisztérium Informatikai Biztonsági Szabályzatát a jelen utasítás mellékletében foglaltak szerint határozom meg.

2. A Belügyminisztérium Igazgatás Reprezentációs Szabályzatáról szóló 13/2010. (XI. 12.) BM utasítás Melléklet 1. pontja helyébe a következő rendelkezés lép:
„1. A szabályzat hatálya a Belügyminisztérium (a továbbiakban: BM) hivatali szervezeteire terjed ki."

3. Az utasítás a közzététele napját követő napon lép hatályba.

Dr. Pintér Sándor s. k.,
belügyminiszter

Melléklet a 29/2010. (XII. 31.) BM utasításhoz

A Belügyminisztérium Informatikai Biztonsági Szabályzata

I. Általános rész

1. A szabályzat hatálya

1. Jelen szabályzat személyi hatálya kiterjed:
   a) a Belügyminisztérium (a továbbiakban: BM) kormánytisztviselőire, ügykezelőire, berendelt vagy vezényelt hivatásos állományú munkatársaira (a továbbiakban: BM munkatárs),
   b) a BM informatikai rendszerével, szolgáltatásaival szerződéses, vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy) a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján.

2. Jelen szabályzat tárgyi hatálya a BM használatában lévő, vagy az általa üzemeltetett valamennyi meglévő és a jövőben fejlesztendő informatikai rendszerre, illetve azok környezetét alkotó rendszerelemekre terjed ki, azok teljes életciklusában (az előkészítéstől a rendszerből történő kivonásig), kivéve a minősített adatokat kezelő rendszereket. A szabályzat tárgyi hatálya nem terjed ki a vezeték nélküli Internet hozzáférés használatra és a nyilvános prezentáció megjelenítő rendszerekre.

2. Alapelvek

3. A BM munkatársának kötelessége az információvédelem területén az adott helyzetben általában elvárható magatartást tanúsítani, és tartózkodni minden károkozó tevékenységtől.

4. Az informatikai eszköz használója csak az a személy lehet, aki a BM munkatársa, a munkavégzéshez szükséges mértékű informatikai ismeretekkel rendelkezik, a jelen szabályzat rendelkezéseit megismerte és a vezetője engedélyével hozzáférési jogosultságot kapott a BM informatikai rendszereihez.

5. Az informatikai rendszer/eszköz működtetése során, a munkaköri leírásban el kell különíteni a jogköröket és a feladatköröket az egyes személyek között annak érdekében, hogy a személyes felelősség megállapítása mindenkor biztosított legyen.

6. Az informatikai rendszert úgy kell kialakítani, hogy biztosított legyen a megbízható működés, az egyes alrendszer vagy rendszerelem funkcionalitásának megfelelő zavartalan és folyamatos működése.

7. A BM objektumában a BM számára létrehozott logikai hálózathoz csatlakozó, vagy a BM által engedélyezett hálózatba nem kötött eszközök (a továbbiakban: eszközök) rendeltetésszerűen, munkavégzés céljából, a BM érdekeinek szem előtt tartásával, a BM által meghatározott módon, a felhasználó felelősségére használhatóak. Az eszközöket ettől eltérő célra – különösen magáncélra – használni nem lehet.

8. A felhasználó felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver és szoftver integritását. Az integritás sérelmének minősül a rendeltetésellenes használat, hardveres vagy szoftveres módosítás.

9. A BM munkatársainak olyan tagja kaphat belépési hozzáférést a BM hálózati alkalmazásaihoz, akinek a munkája azt megköveteli, rendelkezik a munkavégzéshez szükséges mértékű informatikai ismeretekkel, továbbá nyilatkozik jelen szabályzat tudomásul vételéről.

10. Nem lehet más felhasználó azonosítójával a BM hálózatára bejelentkezni, más részére a bejelentkezési hozzáférést átadni.

11. A BM tulajdonát nem képező, idegen információs, számítástechnikai és telekommunikációs eszközt engedély nélkül a BM informatikai struktúrájába csatlakoztatni nem lehet. Kivételt képeznek ez alól az olyan információhordozó eszközök, amelyek munka céljából kerülnek alkalmazásra.

12. Jelen szabályzat alkalmazásában

12.1. adat: az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre, vagy feldolgozásra. Tények, fogalmak vagy utasítások formalizált ábrázolása, amely alkalmas az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra (MSZ ISO 2382-1). A számítástechnikában adat a számítógépes állományok meghatározott része (minden, ami nem program), illetve mindaz, amivel a számítógépek a kommunikációjuk során foglalkoznak (kimenő és bemenő adat);

12.2 adatállomány: az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok;

12.3. adatátvitel: az adatok informatikai rendszerek, rendszerelemek közötti továbbítása;

12.4. adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;

12.5. adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi;

12.6. adatgazda: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki jogosult minősítés vagy osztályba sorolás elvégzésére, felelős az általa kezelt adatokért;

12.7. adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása;

12.8. adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg;

12.9. adattal rendelkezés: a birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás), a minősítés

(biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, a titoktartási kötelezettség alóli felmentés, megismerési engedély kiadása;

12.10. adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

12.11. adatvédelem: az adatkezelés során érintett természetes személyek jogainak és érdekeinek védelmére és az adatkezelés során felmerülő eljárásokra vonatkozó szabályozások és eljárások;

12.12. akkreditálás: olyan eljárás, amelynek során egy erre feljogosított testület hivatalos elismerését adja annak, hogy egy adott szervezet vagy személy felkészült és alkalmas bizonyos tevékenységek elvégzésére;

12.13. alkalmazás, alkalmazói program: olyan program, amelyet az alkalmazó saját speciális céljai elérése érdekében vezet be, és amely a hardver- és az üzemi rendszer funkcióit használja;

12.14. behatolás: védett rendszerbe jogosulatlan belépés a védelem megkerülésével, vagy védelmi hiba kihasználásával;

12.15. bejelentkezés: a felhasználó által kezdeményezett olyan logikai kapcsolat, amelynek eredményeképpen az informatikai rendszer funkcióinak használata lehetővé válik;

12.16. bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

12.17. biztonság: a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg;

12.18. biztonsági esemény: az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, melynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet;

12.19. biztonsági követelmények: A kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese;

12.20. biztonsági mechanizmus: olyan eljárás, módszer vagy megoldási elv – ami lehet számítástechnikai műszaki tartalmú is –, amely valamilyen biztonsági követelmény(eke)t valósít meg;

12.21. biztonsági osztályba sorolás: az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó védelmi szintet meghatározó besorolása, osztályozása;

12.22. elektronikus aláírás: az informatikai rendszerben kezelt adathoz csatolt, kódolással előállított jelsorozat, amely az adat, illetve az eljáró személy azonosságának, hitelességének és sértetlenségének bizonyítására használható;

12.23. érzékeny adat: olyan adat, amely az információbiztonság szempontjából a sérülékenység és a fenyegetettség ténye alá esik (pl. a felhasználás folyamatainak leírása, az eljárás, az adatszerkezetek, vagy az engedélyezési folyamatok);

12.24. felhasználó: személy vagy szervezet, aki (amely) egy adott számítástechnikai eszközt igénybe vesz;

12.25. fenyegetés: a biztonság megsértésének lehetősége;

12.26. fenyegetettség: olyan állapot, amelyben az erőforrások felfedésre, módosításra vagy elpusztításra kerülhetnek;

12.27. funkcionalitás: az informatikai rendszerelem (ideértve az adatot is) tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a felhasználói céloknak megfelel és használható;

12.28. gyenge pont: az informatikai rendszerelem olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

12.29. hálózat: informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége;

12.30. helyreállítás: a katasztrófa következtében megsérült erőforrások eredeti állapotának biztosítása eredeti helyen;

12.31. hitelesítés szolgáltató: egy harmadik személy, amelyet partnerek közössége megbíz azzal, hogy ellenőrizze a kulcsok biztonságos és szakszerű allokációját. Szimmetrikus kulcsrendszerben (szimmetrikus rejtjelező eljárás), ahol mindkét partner ugyanazt a titkos kulcsot használja, a hitelesítő hatóság (Certificate Authority: CA) generálhatja a titkos kulcsot és megküldheti azt a partnereknek. Az aszimmetrikus rendszerben a hitelesítő hatóság generálhatja és küldheti a titkos kulcsot az engedélyezett feladónak, illetve a nyilvános kulcsot a közösség tagjainak;

12.32. hitelesség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik;

12.33. hozzáférés: olyan eljárás, amely valamely informatikai rendszer használója számára elérhetővé tesz a rendszerben adatokként tárolt információkat;

12.34. illetéktelen személy: aki az adat megismerésére nem jogosult;

12.35. információ: tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret (adat), amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg;

12.36. információvédelem: az informatikai rendszerekben kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme;

12.37. informatikai biztonság: az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

12.38. informatikai infrastruktúra: mindazon hardver és szoftver eszközök, informatikai rendszerek, hálózatok, alkalmazások, programok összessége, amelyek segítik és kiszolgálják a szervezet kommunikációs, adatfeldolgozó és adatátviteli tevékenységét;

12.39. informatikai katasztrófaterv: egy katasztrófa bekövetkezése esetén keletkező vagyoni és nem vagyoni kárkövetkezmények elhárítására készített intézkedési terv;

12.40. informatikai rendszer: információs, ügyviteli, üzletviteli vagy egyéb folyamat, szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége. Az informatikai rendszerek közé tartoznak az általános célú számítógépek és a célszámítógépek, de nem soroljuk ide a numerikus vezérlésű eszközöket (pl. robotok, szerszámgépek), a különböző eszközöket vezérlő mikroprocesszoros rendszereket, a processzorvezérelt gépeket (pl. motorelektronika), a zsebszámológépeket és a játékkomputereket;

12.41. Internet: a TCP/IP-protokollon alapuló, nyilvános, világméretű számítógépes hálózat. Az Internet a szolgáltatások széles skáláját nyújtja felhasználóinak (FTP, Gopher, IRC, e-mail, Telnet, http, WWW stb.);

12.42. jelszó: védett karakterfüzér, amelyet a felhasználói névvel együtt használva a belépni szándékozót azonosítja;

12.43. katasztrófaelhárítás-terv: az informatikai rendszer rendelkezésre állásának megszűnése vagy nagymértékű csökkenése utáni visszaállításra vonatkozó terv;

12.44. kiesési idő: az információrendszer leállásától a következő elérési lehetőségig eltelő idő;

12.45. kockázat: a fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat a kárnagyság és a bekövetkezési valószínűség (gyakoriság) szorzata;

12.46. kockázatelemzés: olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési gyakoriságát;

12.47. kódolás: nyílt üzenet kódolása kriptográfiai eljárással, eszközzel vagy módszerrel. A kódolás eredménye a titkosított üzenet;

12.48. kriptográfia: mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak a kutatását, alkalmazását jelenti, amelyek az információ bizalmasságát, hitelességét vagy sértetlenségét hivatottak megvédeni;

12.49. kulcs: a kriptológiában a kódolás és a megfejtés műveleteihez használt szimbólumok sorozata. Az adatbázis-kezelésben egy rekord vagy rekordcsoport azonosítója. A mechanikai védelemben a zárak nyitásához és zárásához használt eszköz;

12.50. kulcsmenedzsment: a kriptográfiában a kódolás és a megfejtés műveleteihez használt kulcsok előállítása, tárolása, szétosztása, törlése, archiválása és alkalmazása, illetve ezek szabályrendszere;

12.51. logikai védelem: az informatikai rendszerben informatikai eszközökkel megvalósított védelem. A logikai védelem fontosabb területei: azonosítás és hitelesítés, hozzáférés-jogosultsági rendszer, hozzáférés-ellenőrzési rendszer, bizonyítékok rendszere;

12.52. megoldás: a kódolt üzenet legális címzettje által, az eljárás ismeretében az eredeti üzenet visszaállítása;

12.53. megszemélyesítés: egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel;

12.54. minősítés: az a döntés, melynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik;

12.55. működésfolytonosság: az informatikai rendszer üzemi működése folytonosságának azon szintje, amely során a kiesési kockázati szint a szervezet számára elviselhető;

12.56. program: a számítógépes utasítások logikailag és funkcionálisan összetartozó sorozata;

12.57. rendelkezésre állás: az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható;

12.58. rendszerelemek: az adatokat körülvevő, az informatikai rendszer részét képző elemek. Rendszerelem-csoportok:
a) az informatikai rendszer környezetét alkotó infrastruktúra,
b) az informatikai rendszer hardverelemei,
c) az informatikai rendszer szoftverelemei,
d) az informatikai rendszer kommunikációs elemei,
e) adathordozók,
f) input és output dokumentumok, az informatikai rendszerre vonatkozó dokumentációk,
g) az informatikai rendszerben részt vevő emberi erőforrások;

12.59. rendszergazda: a számítógépes rendszerek üzemeltetését végző szakember, akivel szemben alapvető feltétel, hogy az informatikai vezető által előírt képesítési követelményeknek megfeleljen;

12.60. rendszerprogram (rendszerszoftver): az operációs rendszer részeként futó program;

12.61. sebezhetőség: A veszélyforrás képezte sikeres támadás bekövetkezése esetén az erőforrások sérülésének lehetősége;

12.62. sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), és a származás megtörténtének bizonyosságát (letagadhatatlanság) is, illetve a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható;

12.63. SSL (Secure Socket Layer): a Netscape által kifejlesztett nyílt szabvány ajánlásbiztonságos kommunikációs csatorna létrehozására a kritikus adatok védelme érdekében;

12.64. szimmetrikus rejtjelező eljárás: a rejtjelezésre és megoldásra egyetlen kulcsot használó rejtjelező eljárás. A megoldó algoritmus nem feltétlenül egy fordított sorrendben végrehajtott rejtjelezés;

12.65. támadás: védett érték megszerzésére, megsemmisítésére, károkozásra irányuló cselekmény. Támadás alatt nem csak a személyek, szervezetek által elkövetett támadásokat, de áttételesen a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is értjük. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő támadási útvonalon zajlik le;

12.66. távmunka: olyan munkavégzés, amely a szervezet épületén kívül történik;

12.67. teljes körű védelem: teljes körű a védelem, ha az informatikai rendszer összes elemére kiterjed;

12.68. üzletmenetfolytonosság-tervezés: az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek;

12.69. vírus: olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg mutálja is önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy „tréfás" hatású kódja is elindul. Többnyire komoly károkat okoz, adatot töröl, formázza a merevlemezt, vagy adatállományokat küld szét e-mailben;

12.70. Warez-oldal: illegális szoftvermásolatok (az eredeti programba épített másolásvédelmet vagy regisztrációt kijátszva/semlegesítve, és ez által bárki számára használhatóvá téve azt) közzétételére fenntartott internetes oldal – warez-site –, ahonnan e programok ingyenesen letölthetők.

II. Biztonsági fokozat

13. A biztonsági osztályok a következők:
a) információvédelmi alapbiztonsági (1.) osztály:
aa) nyílt, jogszabályok által nem védett adatok,
b) információvédelmi fokozott biztonsági (2.) osztály:
ba) személyes adatok,
bb) üzleti titkok,
bc) pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) adatok,
c) információvédelmi kiemelt biztonsági (3.) osztály:
ca) a különleges személyes adatok,
cb) nagy tömegű személyes adatok.

3. Informatikai biztonságpolitika

14. A BM vezetőinek feladata az informatikai rendszerek, valamint az azokban kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának zárt, teljes körű és folytonos, valamint a kockázatokkal arányos védelme, azaz az informatikai biztonság megteremtése, fenntartása. Ennek érdekében a vezetők közreműködnek a szükséges utasítások, rendelkezések, valamint szabályzatok kiadásában, továbbá együttműködnek az Informatikai Biztonságért Felelős vezetővel (17. pont) a védelem adminisztratív, személyi biztonsági, technikai, fizikai, kommunikációs, ellenőrzési rendszerének karbantartásával, kiépítésével és működtetésével kapcsolatos feladatok ellátásában. Ehhez biztosítják hatáskörükhöz mérten a szükséges anyagi, technikai, információs és emberi erőforrásokat.

15. Az informatikai biztonság területén a Közigazgatási Informatikai Bizottság 25. számú ajánlását és a Magyar Informatikai Biztonsági Ajánlásokat kell alkalmazni. El kell készíteni a BM tulajdonában és használatában levő adatvagyon leltárát, fel kell mérni az informatikai elemek érzékenységét.

4. Szervezeti biztonság

16. A biztonsági fórum feladatát a miniszteri értekezlet tölti be. A miniszter a hatáskörét akadályoztatás esetén átadhatja az őt helyettesítő állami vezetőnek. Hatáskörébe tartozik az informatikai biztonság területén:
    a) az informatikai biztonsági irányelvek és feladatok vizsgálata, jóváhagyása,
    b) az információs erőforrások súlyos veszélyhelyzeteknek való kitettségében bekövetkező jelentős változások nyomon követése,
    c) az informatikai biztonsági események nyomon követése,
    d) az informatikai biztonság fokozását szolgáló jelentős kezdeményezések jóváhagyása.

17. Az Informatikai Biztonságért Felelős vezető feladatait az Informatikai Főosztály vezetője (a továbbiakban: Informatikai Biztonságért Felelős vezető) látja el az alábbiak szerint:
    a) általános feladatkörében:
        aa) tervezi, szervezi, irányítja, koordinálja és ellenőrzi a BM-nél üzemeltetetett informatikai rendszerek védelmével összefüggő tevékenységeket, megteremti ezek jogszabályokkal való összhangját,
        ab) külső munkatársakat, szakértőket vonhat be a feladatai ellátásához,
        ac) gondoskodik az informatikai biztonságra vonatkozó jogszabályok, illetve a jelen szabályzat végrehajtásáról, ebben a körben szabályozási koncepciókat, szabályzattervezeteket készít,
        ad) a BM szervezeti egységének megkeresésére, vagy saját hatáskörben szakmai állásfoglalást ad ki,
        ae) az informatikai biztonság szempontjából véleményezi a BM szabályzatait;
    b) az informatikai biztonságot érintő jogi szabályozás területén:
        ba) a jogszabályi változások és a gyakorlati tapasztalatok alapján javaslatokat készít a BM szabályzatainak módosítására,
        bb) kezdeményezi új szabályzatok kiadását,
        bc) gondoskodik az informatikai biztonságra vonatkozó rendelkezések betartásának éves ellenőrzéséről,
        bd) a lefolytatott ellenőrzések, vizsgálatok eredményéről tájékoztatja a BM közigazgatási államtitkárát;
    c) az informatikai biztonság területén:
        ca) felméri és elemzi a BM működéséből eredő, az informatikai biztonsággal összefüggő veszélyforrásokat,
        cb) kidolgozza és döntésre előterjeszti:
            cba) a veszélyforrások felmérése alapján az intézkedési tervet,
            cbb) az informatikai biztonság kialakítására, a megfelelő informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályokat,
            cbc) az informatikai biztonsági tevékenység végzésének személyi, tárgyi, anyagi stb. terveit,
        cc) részt vesz:
            cca) a rendkívüli események kezelésére szolgáló tervek elkészítésében, azok naprakészen tartásában,
            ccb) az informatikai biztonság szempontjából fontosnak minősített munkakörök betöltési szabályainak, feltételeinek meghatározásában,
            ccc) a biztonsági követelmények és az előírások betartásának ellenőrzésében,

cd) véleményezi az informatikai eszközök és alkalmazások beszerzési és fejlesztési igényeit,
ce) tervezi az informatikai biztonságra vonatkozó oktatást,
cf) szükség esetén javaslatokat tesz a megfelelő informatikai biztonsági intézkedésekre, valamint a biztonságos működéssel összefüggő szabályok megváltoztatására,
cg) ellenőrzi az informatikai biztonsági előírások végrehajtását.

18. Az informatikai biztonságpolitika áttekintésének és fejlesztésének koordinálásáért az Informatikai Biztonságért Felelős vezető felel. Ennek érdekében az eredeti szabályozás alapjait érintő minden változás (pl.: új káresemények keletkezése, az informatikai rendszereket veszélyeztető új helyzetek kialakulása, a szervezeti és a műszaki infrastruktúra átalakítása) esetén soron kívüli új vizsgálatot, elemzést végez.

19. Az Informatikai Biztonságért Felelős vezető – az érintettek személyiségi jogainak tiszteletben tartása, és a vizsgálati anyagokhoz minden esetben csatolandó jegyzőkönyv felvétele mellett – jogosult:
    a) a vizsgálati tevékenysége során, a BM tulajdonában és használatában lévő, a munkavégzés céljára kiadott adatbázisba, számítógépes vagy más adathordozó tartalmába betekinteni,
    b) a BM – tulajdonában vagy használatában lévő – helyiségeiben lévő informatikai eszközöket megvizsgálni,
    c) az informatikai rendszerbiztonságot veszélyeztető esemény észlelése esetén az adatkezelési tevékenységgel kapcsolatos azonnali intézkedést jelentési kötelezettség mellett megtenni. Az alkalmazható intézkedéseket a katasztrófaelhárítási terv tartalmazza.

5. Rendelkezés a kapcsolódó szabályozásokról

20. Az Informatikai Biztonságért Felelős vezető az illetéktelen hozzáférés, a károkozás, valamint az adatok jogtalan elérésének megakadályozása érdekében a lehetséges kockázatokat a jelen szabályzatban foglalt alapelvek szerint felméri. Az érintett szervezeti egység vezetője ezen felmérésnek megfelelően biztonsági területeket jelöl ki.

21. Az Informatikai Biztonságért Felelős vezető által megbízott informatikai biztos a jelen szabályzat alapján az alábbi szabályozókat készíti el:
    a) az informatikai biztonságpolitika és stratégia meghatározása,
    b) az informatikai rendszerek biztonsági osztályba sorolása,
    c) az információvédelmi követelmények meghatározása,
    d) az információbiztonsági követelmények meghatározása,
    e) az informatikai működés-folytonossági terv (katasztrófa-elhárítási terv),
    f) az informatikai működési szabályzat,
    g) az informatikai biztonsági kézikönyv,
    h) az informatikai biztonsági szabályzat.

III. A műszaki-technikai, szakmai védelmi intézkedések

6. Infrastruktúrához kapcsolódó védelmi intézkedések

22. A fizikai biztonsági zónákat informatikai rendszerenként, valamint biztonsági osztályonként egyaránt rögzíteni kell. Ez az adott helyiségért és az informatikai rendszerért felelős vezető(k) feladata.

23. A védett helyiségekbe és biztonsági területekre, valamint zónákba való belépési jogosultságokat úgy kell meghatározni, hogy az egyes személyeket, a személyek csoportjait az informatikai rendszerben vagy környezetében betöltött szerepük alapján kell hozzárendelni a helyiségekhez vagy helyiségcsoportokhoz.

24. A BM infrastruktúrája a kormányzat kritikus infrastruktúrájának részét képezi. Az infrastruktúrák biztonsági osztályozását a 13. pont szerint kell kijelölni.

25. Az informatikai rendszerek környezetét megfelelő fizikai, mechanikai, elektronikai és személyi védelemmel kell biztosítani (pl. rácsos ablakok, az áttörést megnehezítő üvegezés, acél ajtók stb.). Az alkalmazott védelmi formák körét, azok kialakítását az Informatikai Biztonságért Felelős vezető határozza meg a Biztonsági Szabályzat előírásainak megtartása mellett, az adott létesítmény védelmi igényének és speciális feltételeinek figyelembevételével.

7. Informatikai eszközt tartalmazó helyiségekbe való belépés rendje

26. Az informatikai rendszer biztonsága szempontjából azokat a helyiségeket és épületeket kell védeni, amelyekben informatikai rendszer működik. A BM használatában lévő épület azon helyiségében, ahol számítástechnikai vagy információs eszközök vannak, csak azok a személyek tartozódhatnak, akik ott dolgoznak. Az ügyintézés céljából jelen levő, vagy külső személyek csak kísérettel és állandó felügyelet mellett tartózkodhatnak a helyiségben.

27. A biztonsági területekre és az egyes biztonsági zónákba való belépést, vagy beléptetést ellenőrizni és naplózni kell.

28. Ha az alap biztonsági területeken, illetve az egyes biztonsági zónákban állandó belépési jogosultsággal nem rendelkező személy tartózkodik, a be- és kilépést minden esetben naplózni kell. A beléptetés előtt ellenőrizni kell a belépő által megjelölt belépési célt.

29. Az olyan helyiségeket, ahol számítástechnikai eszközökkel történik a munkavégzés, biztonsági zárral kell ellátni és a helyiséget távollét esetén zárva kell tartani.

30. A környezeti veszélyek és kockázatok mérséklése érdekében:
    a) a berendezéseket úgy kell elhelyezni, hogy lehetőleg megakadályozzuk az illetéktelen hozzáférést, és a helyiség észrevétlen megközelítését,
    b) a különleges védelmet igénylő fokozott és kiemelt biztonsági osztályba tartozó eszközöket elkülönítetten kell elhelyezni és használni,
    c) a környezeti határok és a lehetséges veszélyforrások folyamatos vizsgálatával és elemzésével kell törekedni a szükséges működési feltételek biztosítására.

8. Központi géptermek védelmi előírásai

31. A központi géptermek a kiemelt biztonsági osztályba tartoznak. Ennek megfelelően a központi hardvererőforrások, az azokon üzemeltetett alkalmazások és kezelt adatok információvédelmének és megbízható működésének biztosításában nagy szerepet játszik az ezeknek helyt adó helyiségek (pl. szerverszobák) védelme.

32. A központi géptermek védelmének az adatok feldolgozását, tárolását, a hálózat működését biztosító berendezések védelmén túl ki kell terjednie a tárolt szoftverek, adatok és dokumentációk védelmére is.

33. A védelemnek az alkalmazások rendelkezésre állásának szükséges mértékével, a hardver és a szoftver beszerzési értékével, az adatok pótlásának költségével kell arányban lennie, a védelem teljes körű és mindenre kiterjedő kell, hogy legyen.

34. A teljes körű védelemről már a helyiségek kialakítása során gondoskodni kell. A védelem egyaránt kiterjed az élőerős, a mechanikai (építészeti) védelemre és a technikai (elektronikai) védelemre.

35. A számítóközpontokba, a szerverszobákba, és az egyéb központi jellegű informatikai helyiségekbe csak az arra jogosult személyek léphetnek be. A belépést minden esetben elektronikusan naplózni kell.

36. Külső személyek beléptetése esetében:
    a) előre kell időpontot egyeztetetni az Informatikai Főosztály képviselőjével,
    b) a személy az adott helyiségben csak kísérettel és szoros felügyelet mellett tartózkodhat,
    c) a helyiségbe idegen számítástechnikai eszközt csak az Informatikai Biztonságért Felelős vezető engedélyével lehet bevinni.

9. Áramellátás szolgáltatási rendje

37. A megbízható működés szempontjából lényeges követelmény, hogy az elektromos hálózatot a szünetmenetességre, az áthidalási és újratöltési időre vonatkozó követelményeknek megfelelően kell kialakítani, és külön leágazás megépítésével kell a betáplálásról gondoskodni. Ha egy nem szerverszobának kijelölt hivatali helyiségben szerver üzemel, gondoskodni kell lokális szünetmentes tápáramellátásról.

38. Az elektromos hálózatnak meg kell felelnie az MSZ 1600 sorozatú szabványoknak. Az érintésvédelemnek meg kell felelnie az MSZ 172 sorozatú szabványoknak.

39. Az elektromos hálózat meghibásodása, az energiaellátás megszűnése esetén gondoskodni kell az informatikai berendezések védelméről, a következők szerint:
    a) az informatikai eszköz üzembentartójának, meg kell felelnie az informatikai berendezés gyártója által meghatározott energiaellátási követelményeknek,
    b) lehetőség szerint megszakítás nélküli áramforrást (UPS) kell használni,
    c) többféle alternatív áramszolgáltatási lehetőséget kell igénybe venni (pl. aggregátor).

40. Az energiaellátó hálózat kábelezésénél:
    a) védett kábeleket kell használni:
       aa) a károkozás, szándékos vagy gondatlan beavatkozás elhárítására,
       ab) a környezeti veszélyek (tűz, robbanás, füst, víz, por, elektromágneses sugárzás) káros hatásai következményeinek elhárítására, csökkentésére.
    b) az adatátviteli (távközlési) kábelt el kell különíteni az energiaellátás kábeleitől.

41. Az elektronikus védelmi rendszert az épület teljes területén, egyedi esetben a mechanikusan is elválasztott fokozott biztonsági osztályba sorolt területen kell kiépíteni. A riasztásoknak az épület biztonsági szolgálatánál, vagy a legközelebbi illetékes rendvédelmi szervnél is meg kell jelenniük. Az elektronikus védelemnek szabotázsvédettnek kell lennie.

10. Telekommunikációs kapcsolódás feltételei

42. A telekommunikációs kapcsolódást, és azok technikai feltételeinek megteremtését a BM használatában lévő épületben a mindenkori szolgáltató végzi. A szolgáltatóval a kapcsolatot az Informatikai Főosztály tartja.

43. Munkavégzéssel kapcsolatos telekommunikációs igényét a felhasználó a munkáltató engedélyével a Központi Szolgáltatási Főigazgatóság felé nyújthatja be. Ilyen igénynek minősül:
    a) a BM használatában lévő épületben a vezetékes vonal esetében a BM-es telefonvonal, a városi vonal, telefonkészülék,
    b) a BM munkatársnak használatában lévő mobiltelefon esetében a BM munkatársi mobil előfizetés, a BM munkatársi mobiltelefon-készülék, a BM munkatársi mobil ügyintézés.

44. A BM informatikai hálózati végpontjának igénybevételét, végpont igénylését, hálózati és alkalmazás hozzáférés igénylését, jogosultságok igénylését az Informatikai Főosztály felé kell benyújtani.

45. Távmunka és távoli asztali elérés érdekében az Informatikai Főosztályvezető hozzájárulásával és a felhasználó közvetlen munkáltatójának írásos engedélyével határozott időtartamra telekommunikációs kapcsolatfelvétel engedélyezhető a BM informatikai hálózatával és azon szolgáltatott alkalmazásokkal. A felhasználó köteles a kapcsolódás technikai feltételeit az Informatikai Főosztály felé jelezni. Az erre a feladatkörre kiadott eszközöket a felhasználó karbantartási, ellenőrzési feladatok ellátása céljából az Informatikai Főosztálynak rendszeresen bemutatja; sérülés, rongálódás esetén anyagi felelősséggel tartozik.

11. Tároló helyiségekre vonatkozó előírások

46. A tároló helyiségeket be kell sorolni a biztonsági osztályoknak megfelelően, attól függően, hogy milyen adatot vagy eszközt kívánunk ott tárolni. Nyílt tárolás esetében a besorolást a helyiség mindenkori használója végzi el.

47. Nyílt tárolás esetén:
    a) elektronikus és papíralapú dokumentumoknál a mindenkori Iratkezelési Szabályzat szerint kell eljárni,
    b) informatikai eszközök munkaidőn túl zárható helyiségben, zártan tárolandóak úgy, hogy csak az arra jogosultak férhessenek hozzá.

48. Zárt tárolás esetén, nyílt adat és adattároló vonatkozásában a Titkosítási és Rejtjelszabályzatban meghatározottak szerint kell eljárni.

49. Speciális biztonsági eszközök alkalmazására az informatikai főosztályvezető engedélyével van mód.

12. Hardverekhez kapcsolódó általános védelmi intézkedések, a felhasználói terminálokra vonatkozó előírások

50. Az informatikai eszközöket, illetve az azokban tárolt, kezelt adatokat védeni kell a jogtalan közzététel, módosítás vagy eltulajdonítás ellen. Fokozottan kell ügyelni a megelőzésre, valamint a megfelelő védelmi intézkedések működtetésére a károk és veszteségek mérséklése érdekében.

51. A monitorokat úgy kell elhelyezni, hogy az azon megjelenő adatokat illetéktelen személy ne láthassa.

52. A képernyővédőket jelszavas védelemmel kell ellátni. A képernyővédő megjelenési idejét úgy kell beállítani, hogy az a rendes munkavégzésben ne okozzon zavart (25 perc).

53. A fokozott, illetve a kiemelt biztonsági osztályba tartozó rendszerek munkaállomásai kizárólag zárolás után hagyhatók felügyelet nélkül.

54. A BIOS-SETUP állítását jelszóhoz kell kötni úgy, hogy annak el kell térnie a felhasználói jelszótól és azt a számítógépet felügyelő rendszeradminisztrátor állítsa be, biztosítva, hogy a felhasználó ne tudja az indítási konfigurációt megváltoztatni.

55. Számítástechnikai eszközöket, adathordozókat, programokat kizárólag a szervezeti egységek vezetőinek írásos engedélyével és az informatikai főosztályvezető hozzájárulásával, meghatározott időtartamra szabad kivinni a munkahelyről a személyi felelősség egyértelművé tételével.

56. A BM területéről kivitt eszközöket a leltárfelelősöknek nyilván kell tartaniuk.

57. A kivitelre kerülő eszközökön tárolt adatok illetéktelenek általi elérhetetlenségére fokozottan kell ügyelni.

58. Meghibásodott eszköz cseréje esetén – garanciális esetben is – adathordozó csak úgy vihető ki, ha arról minden adat visszaállíthatatlan módon törlésre került.

13. Számítógépes hálózati szolgáltatások és az üzemeltetés menedzselése, üzemeltetési eljárások és feladatok

59. Az adatfeldolgozó kapacitások megbízható és biztonságos működésének biztosítása érdekében meg kell határozni az összes adatfeldolgozó egység kezelésére és működtetésére vonatkozó feladatokat és eljárásokat. Ebbe beletartozik az összes szükséges működtetési és hibaelhárítási eljárás elkészítése.

60. Az üzemeltetési eljárásokat az üzemeltetést végző személynek részletesen dokumentálnia kell. Egyedi esetben ezen dokumentálási kötelezettség az üzemeltetést megrendelőt terheli. A dokumentumokat az Iratkezelési Szabályzatnak megfelelően, az Informatikai Főosztályon kell tárolni.

61. Az üzemeltetési eljárások dokumentációinak a munkafolyamat minden részelemének vonatkozásában részletes utasításokat kell tartalmaznia a következők szerint:
    a) az adatkezelés (-feldolgozás, -tárolás, -gyűjtés és -továbbítás),
    b) tervezett követelmények, más rendszerek bizalmasságának sérülése,
    c) munkaidőn kívüli munkahelyen való tartózkodás,
    d) hibaesetekre és rendellenes működésre vonatkozó eljárások,
    e) munkavégzés közben fellépő kivételes állapotok kezelése,
    f) rendszer újraindítása és visszaállítása.

62. Az üzemeltetési eljárások dokumentációját az üzemeltetés helyén hozzáférhetővé kell tenni az érintettek részére.

63. A változásokat ellenőrizni és dokumentálni kell, továbbá a következő tevékenységeket kell elvégezni:
    a) jelentős változások azonosítása,
    b) felelős résztvevők megjelölése,
    c) a változások lehetséges hatásainak felmérése,
    d) a tervezett változtatások jóváhagyási eljárásainak ellenőrzése,
    e) az összes érintett értesítése a változások részleteiről,
    f) a változtatás megszakításáért és az eredeti állapotba való visszaállításért felelős személy kijelölése.

14. A feladatkörök biztonsági szétválasztása

64. Az informatikai rendszerek biztonsági beállításához fűződő tevékenységeket – a véletlen vagy szándékos visszaélések elkerülése érdekében – szét kell választani úgy, hogy azokat több személynek együttesen kelljen végrehajtania. A biztonsági ellenőrzés a végrehajtó szervezettől és a menedzsmenttől függetlenül működik.

65. Ahol a szétválasztás megoldása aránytalan terheket jelentene a szervezetre, ott monitorozással, az eseménynaplók elemzésével és fokozott vezetői felügyelettel kell eljárni.

66. Éles üzemben működtetett informatikai rendszerben fejlesztések, tesztelések a fejlesztési szabályok szerint végezhetők.

67. Fejlesztés alatt álló rendszerben éles üzemi tevékenységet folytatni nem lehet.

68. A fordító-, szerkesztő és egyéb segédprogramok éles üzemi rendszerben csak abban az esetben lehetnek elérhetők, ha ezekre a programokra dokumentáltan és az rendszergazda által engedélyezetten szükség van.

69. A fejlesztők az üzemi rendszerben rendszergazdai (adminisztrátor, root, supervisor stb.) jogosultságokat csak ideiglenesen, a feladatok ellátásához feltétlenül szükséges időre kaphatnak. Ezt követően a jelszavakat haladéktalanul meg kell változtatni, és a rendszer biztonsági beállításait teljes körűen felül kell vizsgálni.

70. Az Informatikai Biztonságért Felelős vezető részére kiadott olvasási jogosultságok csak az adatvédelmi tevékenységgel kapcsolatos munkák során, jegyzőkönyvezve használhatók.

15. Külső létesítmények üzemeltetése

71. A BM informatikai rendszereinek üzemeltetésére, adatfeldolgozására külső személlyel kötött vállalkozási szerződésekben ki kell térni a BM ellenőrzési jogosultságára, lehetőségeire, eszközeire és eljárásaira. A szerződéskötés során figyelembe kell venni:
   a) az alkalmazások és adatok érzékenységét, biztonsági osztályát,
   b) a szükséges jóváhagyások beszerzését,
   c) az üzletmenet-folytonossági (katasztrófaelhárítási) tervekre gyakorolt hatását,
   d) a vállalkozó által alkalmazandó biztonsági szabályokat és alkalmazásokat,
   e) a biztonsággal, valamint az adatkezeléssel összefüggő tevékenységek hatékony nyomon követhetőségét,
   f) a biztonsági események jelentéstételi kötelezettségét, illetve a kezelésükre vonatkozó feladatokat és eljárásokat.

16. Felhasználói előírások

72. A munkaállomások mellé minden szervezeti egységnél egy kezelői útmutatót kell csatolni, amelyet az Informatikai Főosztály készít el.

73. A BM használatában lévő minden egyes rendszernek felhasználói útmutatóval kell rendelkeznie. A kezelői útmutatókban ki kell térni a felhasználói szerepkörök sajátosságaira.

17. Szállítási rend

74. A BM tulajdonát képező informatikai eszköz a BM használatában lévő épületen kívülre az Informatikai Főosztály vezetőjének csomagkiviteli engedélyével szállítható.

75. A BM tulajdonát képező informatikai eszköz a BM használatában lévő épületen belül az Informatikai Főosztály vezetőjének engedélyével szállítható.

76. Minősített adatot tartalmazó rendszerelem, információs hordozóeszköz a minősített adat védelméről szóló 2009. évi CLV. törvényben, illetve BM Biztonsági Szabályzatában meghatározottak szerint, az Informatikai Főosztály vezetőjének jóváhagyásával szállítható.

18. Szoftverekhez kapcsolódó általános védelmi intézkedések, informatikai rendszerek tervezése és átvétele

77. A megfelelő kapacitás és a szükséges erőforrások elérhetősége érdekében előzetes tervezést és előkészületeket kell végrehajtani.

78. A rendszer(ek) túlterheltségével járó kockázatok mérséklése érdekében szükség van a kapacitások iránti várható igények előrejelzésére.

79. Meg kell határozni az új rendszerek üzemeltetési követelményeit, a rendszer átvétele és üzembe helyezése előtt el kell végezni a követelmények dokumentálását, és le kell futtatni a szükséges teszteket.

80. A rendszer működtetéséhez, működéséhez szükséges adatfeldolgozó és adattároló kapacitásokról való gondoskodás során:
   a) fel kell mérni, illetve nyomon kell követni a kapacitás iránti igények várható alakulását,
   b) figyelembe kell venni a környezet és a rendszer támasztotta igényeket,

c) nyomon kell követni a rendszer erőforrásainak – processzorok, központi tárolóegységek, adatállományok tárolására rendszeresített eszközök, nyomtatók és egyéb kimenetek, adatátviteli rendszerek – felhasználását, terhelését,

d) ki kell szűrni és meg kell szüntetni a rendszer biztonságát és a felhasználói szolgáltatásokat veszélyeztető szűk keresztmetszeteket, illetve meg kell tervezni a rendszer helyreállításához szükséges intézkedéseket.

81. Az informatikai rendszerek átvételének alapvető követelménye az átadás-átvételi jegyzőkönyv, melynek tartalmaznia kell minden, az átvétellel kapcsolatos feladatot, kötelezettséget, dokumentációt.

19. Védelem a rosszindulatú programok ellen, vírusellenőrzési mechanizmus előírása

82. Törekedni kell arra, hogy megfelelő intézkedésekkel megakadályozzuk, illetve kiszűrjük a rosszindulatú programokat (vírusokkal fertőzött termékek, a hálózati férgek, trójai lovak, logikai bombák stb.).

83. A felhasználóknak a kötelező oktatás során meg kell ismerniük a rosszindulatú és engedély nélküli programok alkalmazásával járó veszélyeket.

84. Az Informatikai Főosztály vezetője gondoskodik a rosszindulatú programok kiszűrésére és megelőzésére alkalmas különleges ellenőrző eszközök alkalmazásáról, beszerzéséről.

85. A rosszindulatú programokkal szembeni védekezést szűréssel és a programok bevezetése előtti ellenőrzéssel kell megvalósítani. A rosszindulatú program elleni védekezés részét képezi a felhasználók tájékoztatása és oktatása, a hozzáférés-védelem, továbbá a változtatások felügyelete és ellenőrzése. Ennek során szükséges:

a) olyan eszközök alkalmazása, melyek megkövetelik a jogtiszta programok használatát és tiltják az engedély nélküli termékek alkalmazását,

b) külső hálózatokból vagy azokon keresztül, illetve egyéb adathordozókról telepített adatállományok és programok felhasználásával járó kockázat elhárításához szükséges intézkedések bevezetése,

c) rosszindulatú programokat felismerő és megsemmisítő programok telepítése és rendszeres aktualizálása,

d) a kritikus folyamatokat támogató rendszerek adattartalmának és programjainak rendszeres vizsgálata,

e) a bizonytalan eredetű adatállományok ellenőrzése, vírusok kiszűrése,

f) e-mail kiterjesztések, csatolt dokumentumok és letöltések használat előtti ellenőrzése,

g) a vírusokkal szembeni védelemre vonatkozó feladatok és eljárások meghatározása, alkalmazásuk oktatása, a vírustámadások naplózása és az eredeti állapot helyreállítása,

h) megfelelő üzletmenet-folytonossági terv összeállítása, a szükséges adatállományok és programok back-up példányainak és a helyreállítás eljárásainak elkészítése,

i) a hamis, vagy hamisított programra vonatkozó összes információ ellenőrzése, a figyelmeztető tájékoztató kiadványok folyamatos frissítése, meglétének ellenőrzése.

86. Az informatikai üzemeltetés értesíti a felhasználókat a rendszerhibát okozó láncelevelekről illetve az illegális programok használatának veszélyeiről, továbbá folyamatosan figyelmezteti a felhasználókat a frissen megjelent fenyegetésekről. A felhasználót a gépén tárolt illegális programokért felelősségre kell vonni.

87. Központosított hálózati felhasználó adminisztrációt kell kialakítani – az egyenrangú hálózatokat fel kell számolni –, a felhasználókat tartományba kell bejelentkeztetni.

88. Az érintett BM munkatársak felhasználói oktatásának ki kell térni a vírusvédelmi rendszer működésére.

20. Rendszergazdai tevékenységek

89. A megtervezett mentési és visszaállítási eljárásokra üzemeltetési előírásokat kell készíteni, és azok betartását rendszeresen ellenőrizni kell.

90. A biztonsági mentéseket a háromgenerációs elv betartása mellett, lehetőség szerint külön telephelyen, de minimum a követelményeknek megfelelő külön helyiségben kell tárolni. Ennek részletes szabályait az üzletmenet-folytonossági terv határozza meg.

91. A mentések nyilvántartását az előírásoknak megfelelően kell vezetni, és azok helyességét rendszeresen ellenőrizni kell.

92. Az időszakos (pl.: negyedéves) mentéseket 1 évig, az archiválásokat a jogszabályokban meghatározott ideig, de legalább három évig visszakereshetően, helyreállíthatóan kell megőrizni.

93. Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert kell kialakítani, hogy utólag megállapíthatóak legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ellenőrizhetővé kell tenni a hozzáférések jogosultságát, megállapíthatóvá kell tenni a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy annak kísérletét.

94. Az rendszergazdai naplókat legalább 30 napig meg kell őrizni.

95. A BM infrastruktúrájában lévő rendszereknek képesnek kell lenniük minden egyes felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A minimálisan kötelezően regisztrálandó események a következők:
    a) rendszerindítások, -leállások, -leállítások,
    b) rendszerhibák és korrekciós intézkedések,
    c) programindítások és -leállások, -leállítások,
    d) az azonosítási és hitelesítési mechanizmus használata,
    e) hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,
    f) az adatállományok és kimeneti adatok kezelésének visszaigazolása,
    g) azonosítóval ellátott erőforrás létrehozása vagy törlése,
    h) felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.

96. A BM infrastruktúrájában lévő rendszer üzemeltetése során rendszergazdai naplót kell vezetni, amelyet az Informatikai Főosztály vezetője és az Informatikai Biztonságért Felelős vezető rendszeresen ellenőriz.

97. Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.

98. Az informatikai rendszer üzemeltetéséről nyilvántartást kell vezetni, amelyet az Informatikai Biztonságért Felelős vezető rendszeresen ellenőriz.

99. Az üzemzavarok elhárítása érdekében, a bejelentést követően korrekciós intézkedéseket kell kezdeményezni. A felhasználók által jelentett, az adatfeldolgozás vagy átviteli rendszerek működésében észlelt hibákat naplózni kell.

100. Az üzemzavar kezelésének szabályai:
    a) a hibanapló vizsgálata és a hiba kezelésének, elhárításának ellenőrzése,
    b) korrekciós intézkedések vizsgálata, illetve ezek végrehajtásának és a kezdeményezett intézkedések engedélyezése engedélyezésének szabályosságának ellenőrzése.

21. Hálózatmenedzsment

101. A hálózatmenedzsment segítségével kell meghatározni a hálózatok adattartalmának biztonságát és az infrastruktúra védelmét, különös tekintettel a több szervezetet átfogó hálózatokra.

102. A BM közvetlen szervezeti és fizikai felügyeletén kívül eső kapcsolatok esetében a kriptográfiai módszerek (kódolás, digitális aláírás, SSL/TSL, https stb.) használata kötelező.

103. A 102. pont szerint alkalmazandó kriptográfiai módszert az Informatikai Biztonságért Felelős vezető választja ki és hagyja jóvá.

104. Olyan ellenőrző eszközökről kell gondoskodni, amelyek biztosítják a hálózatokban kezelt és továbbított adatok – a biztonsági osztálynak megfelelő – biztonságát, valamint a kapcsolt szolgáltatásokat megóvják az illetéktelen hozzáférésektől.

105. A hálózatok és a számítógépek működtetésének feladatait szét kell választani.

106. A nyilvános hálózatokon keresztül továbbított adatok, illetve a kapcsoltrendszerek védelmére pótlólagos ellenőrző eszközökre van szükség.

107. Pontosan definiálni kell a hálózat határait. A hálózat biztonságos szegmentálásának kialakításáért az Informatikai Főosztály vezetője a felelős.

108. Az informatikai rendszerek dokumentációja biztonságilag érzékeny adatokat is tartalmazhat. Ilyen érzékeny adat lehet a felhasználás folyamatainak leírása, az eljárás, az adatszerkezetek, vagy az engedélyezési folyamatok ismertetése.

109. Az illetéktelen hozzáférés megelőzése érdekében:
   a) gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról;
   b) minimálisra kell csökkenteni a rendszerdokumentációkhoz hozzáférők számát;
   c) gondoskodni kell a nyilvános hálózaton keresztül elérhető, vagy azon keresztül továbbított dokumentáció védelméről;
   d) az informatikai rendszer biztonságával kapcsolatos dokumentációt az informatikai rendszer biztonsági fokozatának megfelelő módon kell kezelni;
   e) az informatikai rendszer (vagy annak bármely elemének) dokumentációját változások menedzselésének keretében kell naprakészen tartani;
   f) gondoskodni kell a változások menedzseléséről és a biztonságot érintő változások, változtatások naplózásáról;
   g) a rendszerben feldolgozásra kerülő, a fokozott és a kiemelt biztonsági osztályba sorolt adatok és a hozzájuk kapcsolódó jogosultságok nyilvántartását elkülönítetten kell kezelni;
   h) az informatikai rendszer beszerzéssel vagy fejlesztéssel történő kialakításához és üzemeltetéséhez, a rendszer funkcionalitásának és megbízható üzemeltetésének a biztosításához a következő dokumentációk szükségesek:
      ha) rendszerterv,
      hb) üzembe helyezési jegyzőkönyv,
      hc) katasztrófa-elhárítási terv,
      hd) üzletmenet-folytonossági terv;
   i) a biztonsági rendszerek, alrendszerek dokumentációjának tartalmaznia kell a biztonsági funkciók leírását, azok installációját, aktiválását, leállítását és használatát a fejlesztés, valamint az üzemeltetés során. Biztonsági rendszer, alrendszer dokumentációját csak az Informatikai Biztonságért Felelős vezető által engedélyezett személyek kezelhetik.

22. Az elektronikus levelezés biztonsága

110. Az elektronikus levelezés biztonságának szabályozásakor a következő fenyegetettségeket kell figyelembe venni:
   a) az üzenetek illetéktelen elérésének vagy módosításának, illetve a szolgáltatás megtagadásának veszélye;
   b) emberi hibákból eredő veszélyeztető tényezők (pl. rossz címzés vagy irányítás);
   c) érzékeny adatok továbbításának lehetősége és ennek veszélyei;
   d) a feladó- és címzetthitelesítési problémák, illetve a levél átvételének bizonyítása;
   e) a kívülről hozzáférhető címjegyzékek tartalmával való visszaélési lehetőségek;
   f) távolról bejelentkező felhasználó biztonsági problémái.

111. Az elektronikus levelezés biztonsági irányelvei:
   a) a levelezőrendszer vírusvédelmét folyamatosan frissíteni kell, valamint követni kell az új mail vírusok megjelenését;
   b) az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell (pl. nyomon kell követni az új szoftverfrissítések, service packok és security-patch fájlok megjelenését);
   c) az elektronikus levelező rendszeren keresztül történő támadások esetén, amennyiben a rendszer védelme átmenetileg nem biztosított – pl. olyan vírusfenyegetettség esetében, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet –, a belső hálózaton (intraneten) kívül eső elektronikus levélforgalmat ideiglenesen le kell állítani. Ennek elrendelésére az Informatikai Biztonságért Felelős vezető jogosult;
   d) definiálni kell a felhasználók felelősségét a minisztérium érdekeinek védelmében;
   e) az elektronikus üzenetek bizalmasságának, illetve hitelességének védelme érdekében használt kriptográfiai eszközt vagy eljárást az Informatikai Biztonságért Felelős vezető engedélyez;
   f) kilépéskor archiválni kell és a kilépés napjától számított 30 napig meg kell őrizni minden olyan felhasználó elektronikus levelezését, akiknek munkaviszonya, illetve a jogosultság alapját képező megbízása, szerződése megszűnt. Megőrizendők továbbá azok az elektronikus levelek, amelyek fegyelmi, büntető vagy polgári eljárások alapját képezhetik az eljárás befejezéséig;
   g) a nem hitelesíthető, kétes forrásból származó üzeneteket ki kell vizsgálni, az elektronikus levelezés forgalmát – a technikai lehetőségek szerint – tartalmilag szűrni kell, a bizalmas adatok kiszivárgásának elkerülése érdekében, minden felhasználót fel kell világosítani arról, hogy a BM levelezőrendszerén tárolt és továbbított levelek, a BM tulajdonát képezik, ezért a BM szabályzatokban és utasításokban feljogosított ellenőrző szerveinek ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van;
   h) a BM levelezőrendszere reklám, valamint egyéb üzleti célokra nem használható.

112. A levelezőrendszer elérése csak védett (hiteles és kódolt) csatornán (pl. https) keresztül valósítható meg. A hozzáférés csak jelszavas védelmen keresztül történhet. A felhasználó felügyeleti lehetőségein kívüli (például nyilvános, idegen tulajdonú) munkaállomások, terminálok használata esetén csak az ennek megfelelő üzemmódban szabad bejelentkezni.

113. A BM elektronikus levelezési címjegyzéke nem szolgáltatható ki külső személynek.

23. Irodaautomatizálási rendszer, alkalmazói programok

114. Az automatizált irodai rendszerek olyan komplex tevékenység elősegítésére jöttek létre, amelyek egyaránt tartalmazzák a dokumentumok, hangok és képek elektronikus eszközökkel való előállítását, kezelését, tárolását, valamint továbbítását. Az automatizált irodai rendszerekben használt eszközök (asztali és mobil számítástechnika, hangátvitel, multimédia stb.) összekapcsolása során több, egymással összefüggő biztonsági követelményt kell mérlegelni:
   a) a továbbított és felhasznált adatok sebezhetőségének figyelembevétele;
   b) az adatok minősítésük szerinti kezelése, a biztonsági osztályba sorolásnak megfelelő védelmi követelmények teljesítése, illetve betartásuk ellenőrzése az adatgazda feladata;
   c) a felhasználók hozzáférési jogosultságainak meghatározásánál, kiosztásánál és használatuk ellenőrzése során figyelembe kell venni a jelen szabályzat előírásait;
   d) a biztonsági naplófájlokat a rendszer biztonsági osztályának megfelelő módon kell kezelni és kiértékelni. Az észlelt eltéréseket (hibás kezelés, jogosultság megsértése stb.) haladéktalanul ki kell vizsgálni, és a vizsgálat eredményét jegyzőkönyvezni kell. Ezekért az adott szervezeti egység vezetője a felelős;
   e) az érzékeny adatok védelmének a biztosítása (jogosultságok, hozzáférés, adatkezelés stb.);
   f) a biztonsági másolatokat, mentéseket a rendszerre előírt módon kell kezelni és tárolni;
   g) az irodaautomatizálási rendszer által kezelt adatbázisokat, használt eszközöket (szerverek, munkaállomások, adattárak, hálózatok) az illetéktelen fizikai hozzáférés ellen is védeni kell.

115. Minden felhasználónak kötelező a biztonságot támogató programokat használni. Az általa használt munkaállomásról a programot nem törölheti le, nem kapcsolhatja ki.

116. Nem munkavégzés célú programokat használni nem lehet.

24. Nyilvános rendszerek használatának rendje

117. Nyilvános rendszerben (pl. egy Interneten keresztül elérhető webszerveren) a fokozott integritást igénylő számítástechnikai programok, adatok és egyéb információk védelméhez megfelelő eszközökre – pl. digitális aláírás alkalmazására – van szükség. Az elektronikus hirdető rendszereknél – különösen azoknál, amelyek lehetővé teszik a visszajelzést és az információ közvetlen beléptetését – megfelelő eszközökkel kell gondoskodni a következőkről:
   a) az információ megszerzésének módja feleljen meg a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rendelkezéseinek,
   b) időben kerüljön sor a rendszerbe bekerülő információ pontos és hiánytalan feldolgozására,
   c) az adatok kezelése (gyűjtés, tárolás, feldolgozás) során gondoskodni kell az adatok, valamint az informatikai rendszerek védelméről,
   d) a rendszerhez való külső hozzáférés ne tegye lehetővé az illetéktelen hozzáférést azokhoz a belső hálózatokhoz, amelyekhez a rendszer csatlakozik.

25. Az Internet használatának rendje

118. Az Internetszolgáltatás a felhasználói jogosultság része.

119. Az internetes hozzáférés igénybevételére csak munkaköri feladatok ellátása érdekében van lehetőség, a hozzáférést személyes célra igénybe venni nem lehet.

120. Az BM által üzemeltetett hálózaton keresztül internetes hozzáféréssel rendelkező felhasználók esetén az igénybevétel jogszerűségének ellenőrzésére az Informatikai Főosztály jogosult. Amennyiben az ellenőrzés során nem indokolható Internethasználatot észlel, erről soron kívül tájékoztatja az érintett felhasználót és az érintett felhasználó közvetlen vezetőjét.

121. Amennyiben az Informatikai Főosztály ismétlődően visszatérő és nyilvánvalóan indokolatlan Internethasználatot észlel, felfüggesztheti a hozzáférési jogosultságot. A felfüggesztéssel egy időben ezen intézkedéséről soron kívül tájékoztatja az érintett felhasználót, a felhasználó közvetlen vezetőjét.

122. A 121. pontban foglalt tájékoztatás alapján a felhasználó közvetlen vezetője dönt az Internet igénybevételi lehetőségének megszüntetéséről, és erről soron kívül tájékoztatja az Informatikai Főosztály vezetőjét.

123. Az igénybevétel jogszerűségének, illetve jogszerűtlenségének megállapítására irányuló eljárás során az érintettnek lehetőséget kell adni arra, hogy a szakmailag indokolatlannak tűnő Internethasználat munkaköri feladatainak ellátásához szükséges voltát bizonyítsa.

124. A BM által biztosított e-mail címet csak munkakörének ellátásához kapcsolódó regisztrációs folyamatokhoz használhatja.

125. Az Informatikai Főosztály a BM hálózati infrastruktúráját és a folyamatos üzemmenetet veszélyeztető hálózati műveleteket korlátozhatja, vagy letilthatja.

126. Nem lehet a BM hálózati infrastruktúráját veszélyeztető oldalakat (felnőtt tartalmú-, warez-, fájlcserélő weboldalak stb.) látogatni.

127. Azoknak a felhasználóknak, akiknek a munkaköréhez tartozóan indokolt a 126. pontban meghatározott oldalak látogatása, külön igény alapján az Informatikai Főosztály biztosítja a hozzáférés körülményeit.

26. Új rendszerprogramok bevezetésének rendje

128. Minden új rendszerprogram-tervezetet meg kell küldeni az Informatikai Főosztálynak véleményezésre.

129. Rendszerprogramot csak az Informatikai Főosztály vezetőjének engedélyével lehet bevezetni.

130. Minden rendszerprogram bevezetésének feltétele, hogy rendelkeznie kell rendszertervvel, rendszerleírással, műszaki leírással, kapcsolódó eszközök leírásával, kezelői útmutatással és oktatói dokumentációval.

131. A rendszer bevezetése és oktatása az Informatikai Főosztály közreműködésével hajtható végre.

27. Adathordozókhoz kapcsolódó általános védelmi intézkedések

132. Az eszközök károsodásának megelőzése, és a tevékenységben okozott fennakadás megakadályozása érdekében:
   a) gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről;
   b) meg kell előzni a dokumentumok, a számítástechnikai adathordozók (szalagok, lemezek, kazetták stb.), az input/output adatok és a rendszerdokumentációk károsodását, eltulajdonítását és engedély nélküli törlését;
   c) szabályozni kell az adathordozók beszerzését, tárolását és kezelését;
   d) biztosítani kell, hogy az adathordozók kezelése – a vonatkozó iratkezelési szabályok szellemében – a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos módon történjék. Az adathordozókról és azok tartalmáról nyilvántartást kell vezetni;
   e) a BM-en kívüli adatforgalomban használt adathordozók előállítása, kiadása és fogadása dokumentált és ellenőrzött módon történhet. Az adathordozókat használatba venni csak az előírt ellenőrző eljárások (pl. vírusellenőrzés) elvégzése után szabad;
   f) minden adathordozót újraalkalmazás előtt, vagy selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell;
   g) az adattípus (minősítés) felismerhető jelölését a számítástechnikai berendezéssel előállított adattároló és megjelenítő eszközökön biztosítani kell;
   h) az adatok sértetlen és hiteles állapotának megőrzését biztosítani kell;
   i) az objektumot elhagyó adathordozón szereplő adatokat minden esetben titkosítási eljárással kell védeni.

133. Az iratkezelés által érintett adathordozókat biztonságos módon kell kezelni a BM Iratkezelési Szabályzat és a BM Biztonsági Szabályzat előírásainak megfelelően.

134. Az adathordozókat – azokat is, amelyek használaton kívül vannak – biztonságos helyen kell tárolni, vagy amennyiben munkaközi példányok, azokat vagy helyreállíthatatlanul törölni kell, vagy meg kell semmisítenie az adathordozó birtokosának, és arról jegyzőkönyvet kell készítenie az Iratkezelési Szabályzatnak megfelelően. Adathordozók:
   a) a kinyomtatott dokumentumok,
   b) a hang- vagy egyéb adatrögzítések,
   c) a kimeneti jelentések,
   d) az egyszer használatos nyomtatószalagok,
   e) a mobil diszkek és kazetták, mágnesszalagok,
   f) a CD, DVD vagy más tárolóeszközök (pendrive, rádiótelefon, memóriakártya stb.),
   g) a programlisták,
   h) a tesztadatok,
   i) a rendszerdokumentáció.

135. Az érzékeny adatokat, mentéseket, archiválásokat tartalmazó adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 perces tűzállósági tároló szekrényben történhet.

136. Az adatok illetéktelen közzétételének, illetve felhasználásának megakadályozása érdekében szükségesek az adatkezelést szabályozó eljárások. Ezeknek az eljárásoknak – az adatok érzékenységének megfelelően – igazodniuk

kell az előírásokhoz, szabályzatokhoz, számítástechnikai rendszerekhez, hálózatokhoz, a használt számítástechnikai eszközökhöz, távközlési, hangátviteli és multimédiás stb. rendszerekhez, levelezőrendszerhez, az informatikai szolgáltatásokhoz. Az adatkezelési eljárások előírása, meghatározása során a következőket kell figyelembe venni:

a) az összes adathordozó kezelése és címkézése,
b) az illetéktelen személyek kiszűrése, hozzáférésük megakadályozása,
c) a bemenő adatok teljes körűségének, az adatfeldolgozás teljességének és a kimeneti adatok hitelességének és hitelesítésének ellenőrzése,
d) a be- és kimenő adatok védelme, a védettség mértékének az adatok érzékenységéhez való igazítása,
e) az adatok elosztásának szabályozása, ellenőrzése és korlátozása,
f) az adatok minősítési szintjét, kezelési jelzését kötelezően alkalmazni kell, és a változásokat automatikusan naplózni kell,
g) rendszeresen ellenőrizni kell az adatok minősítési szintjének alkalmazását,
h) a biztonsági naplófájlokat az arra feljogosított személynek a rendszer minősítésének megfelelő, meghatározott módon kell kezelnie, illetve kiértékelnie,
i) az észlelt eltéréseket (hibás kezelés, jogosultság megsértésének a kísérlete) haladéktalanul ki kell vizsgálni, és az eredményt jegyzőkönyvben kell rögzíteni. Ezért az adott szervezeti egység vezetője a felelős.

28. Adatok és programok átadása

137. A szervezetek között cserélt adatok és programok elvesztésének, módosításának vagy illetéktelen felhasználásának lehetőségét is meg kell akadályozni. Az adatok és a programok szervezetek közötti átadását, cseréjét ellenőrizni kell.

138. Mérlegelni kell az elektronikus adatcsere, az elektronikus kereskedelem és az e-mail biztonsági kockázatát, annak következményeit és az ellenőrző eszközök alkalmazására vonatkozó követelményeket.

139. A BM más szervezettel adat- és programcserét kizárólag írásos nyilatkozat (szerződés, megállapodás stb.) alapján bonyolíthat, amelyben utalni kell az érzékeny információk kezelésére is.

140. A csere biztonsági feltételeire vonatkozó megállapodásokban meg kell határozni:
a) az adatátvitel, -feladás, -fogadás és -átvétel ellenőrzésének és bejelentésének eljárási szabályait,
b) az adatok biztonságos átvitele előkészítésének és tényleges átvitelének műszaki szabványait,
c) adatvesztéssel kapcsolatos kötelezettséget és felelősséget,
d) az adatátvitel során a biztonságos (szükség esetén kódolt) környezet előírásait minden érintett félnél,
e) az érzékeny adatok védelméhez szükséges speciális eszközök igénybevételét (pl. kriptográfiai kulcsok).

141. Az adat, illetve az abból megismerhető információ a fizikai szállítás során történő átvitel esetén ki van téve az illetéktelen hozzáférés és visszaélés veszélyének. A számítástechnikai adathordozók biztonságos szállítása érdekében az alábbi ellenőrző eszközök alkalmazását kell mérlegelni:
a) szállítást – épületen kívül – csak a szervezeti egység vezetője rendelhet el,
b) szállítás során átadás-átvételi bizonylat szükséges,
c) szállítást – lehetőség szerint – több embernek kell végeznie,
d) épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell kiválasztani,
e) tömegközlekedési eszközön – lehetőség szerint – adathordozó nem szállítható,
f) épületen kívüli szállítás esetén megfelelő tárolóeszköz szükséges,
g) elektronikusan rögzített adatokat tartalmazó mágneses adathordozó szállításakor kerülendő a nyilvánvalóan erős mágneses tér megközelítése (pl. nagyfeszültségű távvezetékek, transzformátorház stb.),
h) a szállítás során a vagyonbiztonság érdekében fokozott figyelemmel kell eljárni,
i) az adathordozót nem lehet őrizetlenül hagyni,
j) az adathordozókat óvni kell a fizikai sérülésektől,
k) az adathordozókon a minősítési szintet megváltoztathatatlanul kell feltüntetni.

142. Rendkívüli esemény esetén a szervezeti egység (a szállítást elrendelő) vezetőjét – szükség esetén a rendőrséget is – értesíteni kell. A vezetőnek haladéktalanul meg kell tennie a további károk elkerülése érdekében a szükséges lépéseket, valamint ezzel egy időben tájékoztatnia kell az Informatikai Biztonságért Felelős vezetőt az eseményről és a megtett intézkedésekről.

143. Az elektronikus szolgáltatások biztonsága komplex védelmet igényel, mert az adatkezelés során adatcserére és nyilvános hálózat igénybevételére egyaránt sor kerül(het).

144. A hatékony védelem megvalósítására integrált biztonsági rendszert kell kialakítani, melynek legfontosabb feladatai:
a) a hozzáférés egységes szabályozása és ellenőrzése,
b) egységes azonosítás és hitelesítés (SSO),
c) az elektronikus aláírások kezelése, kódolás, kulcsmenedzsment (CA, PKI),
d) biztonságos adattovábbítás,
e) a behatolási kísérletek figyelése (IDS),
f) biztonsági naplózás a hozzáférések, az azonosítás és a hitelesítés ellenőrzéséhez,
g) az auditálhatóság.

145. Az elektronikus szolgáltató rendszerek hatékony védelmének kialakításához pontosan meg kell határozni a lehetséges fenyegetéseket, a potenciális veszélyeket és a várható támadási módszereket.

29. Az adatcsere egyéb formái

146. Megfelelő eljárásokkal és ellenőrző eszközökkel gondoskodni kell a távközlési és adatátviteli eszközökön keresztül kicserélt információk védelméről. Az információ nem biztonságos felhasználásának lehetséges okai: a szükséges ismeretek hiánya, az ilyen eszközök használatára vonatkozó irányelvek és eljárások nem kellő ismerete.

147. Figyelembe kell venni azt az eshetőséget is, hogy a távközlési eszközökben bekövetkező üzemzavar, az eszközök túlterheltsége vagy a kapcsolat kimaradása esetén a folyamatos üzletmenet megszakadhat, valamint illetéktelen személyek is hozzáférhetnek a különböző információkhoz.

148. Tekintettel arra, hogy belső adatok nem hozhatók nyilvánosságra, a BM munkatársa az adatátviteli eszközök használata (különösen telefonbeszélgetések) során köteles ügyelni:
a) különösen mobiltelefon használata során a közvetlen környezetében tartózkodó emberekre;
b) a telefonbeszélgetések – illetve a készülékek – lehallgatására és letapogató eszközök, vevőkészülékek alkalmazására;
c) a hívott félnél tartózkodó személyekre;
d) arra, hogy ne folytasson bizalmas telefonbeszélgetéseket nyilvános helyen vagy nyitott irodában;
e) arra, hogy ne tároljon feleslegesen üzenetet az üzenetrögzítő készülékeken, illetve nyilvános rendszereken, mert ezeket illetéktelen személyek visszajátszhatják, elolvashatják. Ezeket megismerés után le kell törölni, vagy biztonságos helyen kell tovább tárolni.

149. A faxgépek használata során a következőkre kell tekintettel lenni:
a) a dokumentumok és üzenetek – esetleges – téves számra való elküldése,
b) a gépek szándékos vagy véletlen programozása egy meghatározott címre szánt üzenetek továbbítására,
c) illetéktelen hozzáférés a beépített üzenettárolókhoz, az üzenetek visszakeresése és lehallgatása.

150. Az adathordozókkal kapcsolatos további szabályozásokat kell bevezetni a biztonsági szabályzatban az alábbi területeken:
a) biztonsági másolatok készítésének és tárolásának rendje,
b) munkamásolatok készítési és tárolási rendje,
c) titkosítási célra felhasználható adathordozók használata.

30. Dokumentumokhoz kapcsolódó védelmi intézkedések, az informatikai rendszerek informatikai biztonsági követelményei

151. Az informatikai rendszerek (infrastruktúra, alkalmazások és a felhasználó által kifejlesztett alkalmazások) integrált biztonságát a biztonságpolitikai szempontok szerint kell kialakítani. A biztonság egyik feltétele az alkalmazást vagy szolgáltatást támogató folyamat megtervezése és megvalósítása. Az informatikai rendszerek kifejlesztése előtt meg kell határozni és egyeztetni kell a biztonsági követelményeket az Informatikai Biztonságért Felelős vezetővel.

152. Egy projekt követelményeinek megfogalmazása során meg kell határozni az összes biztonsági követelményt. Ezeket a követelményeket és szükséges megoldásokat egy informatikai rendszer fejlesztésének részeként kell megindokolni, egyeztetni és dokumentálni. A projektek során az informatikai biztonsági előírásokat kell érvényesíteni.

153. A BM informatikai beruházásainak előkészítésére vonatkozó utasításainak figyelembevételével – az informatikai biztonsággal kapcsolatban – a következőknek kell szerepelnie az elkészítendő dokumentum(ok)ban:
   a) az informatikai rendszer által kezelendő adatoknak az információvédelem és a megbízható működés szempontjából történő elemzése, a védelmi célkitűzések meghatározása,
   b) az informatikai rendszer érzékenysége,
   c) a jogszabályokból és a belső szabályozásból eredő kötelezettségek bemutatása,
   d) a fizikai és a logikai védelem rendszer szintű bemutatása,
   e) a megvalósításhoz szükséges feltételrendszer meghatározása,
   f) a biztonsági rendszer teljes költségének becslése, ennek összehasonlítása a lehetséges kockázatokkal, károkkal.

154. Az informatikai biztonsági fejezetnek a tervezési dokumentumokba történő beállításáért a projektvezető, annak kijelöléséig, vagy hiánya esetén az előterjesztő a felelős.

155. A BM minden informatikai projekt előterjesztésének tartalmaznia kell a létrehozandó (fejlesztendő, átalakítandó) informatikai rendszer fizikai, logikai és adminisztratív védelmi rendszerének – a projekt keretében történő – tervezési és megvalósítási lépéseit, költségeit, felelőseit. Az informatikai projekt költségvetésében szerepeltetni kell a biztonsági rendszer tervezési és megvalósítási költségeit.

156. A 155. pontban előírt feltételek hiánya esetén informatikai projekt nem indítható el, amiért a projektvezető a felelős.

31. Biztonság a felhasználói rendszerekben

157. A felhasználói rendszerek integrált biztonsága kiterjed a rendszerekben tárolt felhasználói adatok illetéktelen hozzáférésének, módosításának, törlésének, nem megfelelő felhasználásának stb. megelőzésére. A rendszertervek összeállítása során mérlegelni kell a rendszerbe beépítendő automatikus ellenőrző eszközök, valamint a biztonságot támogató manuális ellenőrző eszközök szükségességét.

158. A felhasználói rendszerek biztonságát a következő intézkedések szavatolják:
   a) a felhasználói rendszerekben – többek között a felhasználó által kifejlesztett alkalmazásokban – meg kell tervezni a megfelelő ellenőrző eszközöket és eseménynaplókat, valamint a tevékenységek naplózását. Ezeknek tartalmazniuk kell a bemenő adatok, a belső adatfeldolgozás és a kimenő adatok hitelesítését,
   b) a biztonsági intézkedéseket pontosan, minden részletre kiterjedően dokumentálni kell,
   c) az adatfeldolgozó rendszerekben bevitt adatokat hitelesíteni, ellenőrizni kell.

159. A bemenő adatok ellenőrzésének eszközei:
   a) az ismételt adatbevitel és az ebből származó adat-karbantartási anomáliák elkerülésére írt eljárások,
   b) időszakos adatmező- és adatállomány-vizsgálat, valamint a felvitt adatok hitelességének, valamint integritásának ellenőrzése és igazolása,
   c) az adatbevitel alapját képező nyomtatott input dokumentumok ellenőrzése, illetve ezek engedély nélküli módosításának megakadályozása, valamint az engedélyezés kikényszerítésére írt eljárások,

d) az adathitelesítési hibák kiküszöbölését elősegítő eljárások,
e) adatbevitel során, a mezőtípus kompatibilitást biztosító, illetve adattartalom helyességét ellenőrző és kikényszerítő eljárások és függvények,
f) az alkalmazáshoz történő hozzáférés naplózása,
g) a feldolgozásban részt vevő BM-munkatársak feladatkörének és felelősségének rögzítése a munkaköri leírásokban.

160. A pontosan és hiánytalanul bevitt adatok biztonságát, integritását a feldolgozás ideje alatt a következő intézkedésekkel kell szavatolni:
a) az adatfeldolgozás rendszerébe ellenőrzési, hitelesítési pontokat kell beépíteni, különös tekintettel az adatmódosító, adattörlő funkciók helyére,
b) adatfeldolgozási hibák esetén: hibadetektáló, és a további rendszerfutást leállító eljárások beépítése a rendszerbe,
c) korrekciós programok alkalmazása a feldolgozás során felmerülő hibák korrigálására,
d) a folyamatba épített ellenőrzés ellátásáért az Informatikai Biztonságért Felelős vezető a felelős.

161. Az üzenethitelesítés, valamint az elektronikus aláírás kialakítása során:
a) az azonosítás és a hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni,
b) a hitelesítés legáltalánosabb módja a jelszó megadása. Kezelésére a jelszókezelésre vonatkozó fejezetben részletezett általános szabályokat kell alkalmazni,
c) a hitelesítést a felhasználó és a rendszer között egy, a felhasználó által megnyitott, védett csatornán keresztül kell biztosítani.

162. Nyilvános kulcs infrastruktúra (Public Key Infrastructure: PKI) alkalmazása során a felelős vezetőnek ki kell alakítania tanúsítványpolitikát (Certificate Policy, CP), melyet az Informatikai Biztonságért Felelős vezetővel egyeztetnie kell. A tanúsítványpolitika alkalmazása kötelező.

163. Az adatfeldolgozás rendszerében ellenőrizni, hitelesíteni kell a kimenő adatokat. Ennek során a kimenő adatok biztonsága érdekében a következő védelmi eljárásokat kell alkalmazni:
a) integritás-ellenőrzés,
b) az adattartalom meglétének, értékének ellenőrzése,
c) a megfelelő minősítés meglétének ellenőrzése,
d) a kimenő adatok értékelésében és hitelesítésében részt vevő BM-munkatársak feladatainak és felelősségének meghatározása a munkaköri leírásokban.

32. Dokumentumok kezelési és tárolási rendje

164. A rendszerleírásokat és rendszerprogram dokumentációkat a rendszerben megjelenő adatok minősítési szintjének megfelelően be kell minősíteni mint dokumentumot. Ezen dokumentumokat a hatályos Biztonsági Szabályzatnak megfelelően kell kezelni és tárolni. Csak olyan rendszer használható a BM használatában lévő épületen belül, amely rendszerleírással rendelkezik.

165. Minden egyes rendszer, vagy alkalmazás a BM szervezetén belül felhasználói dokumentációval kell, hogy rendelkezzen. Ezen dokumentumokat, a rendszer minősítési szintjének megfelelően kell biztonsági osztályokba sorolni, azok kezelését és tárolását az iratkezelés szabályai szerint kell alkalmazni.

166. Elektronikus dokumentum a BM felelősségvállalása mellett, biztonságosan csak a felhasználó szervezete által használt közös hálózati meghajtón, vagy a felhasználó saját hálózati könyvtárában tárolható. Saját hálózati könyvtárat minden felhasználó az Informatikai Főosztálytól kaphat.

33. Adatokhoz kapcsolódó védelmi intézkedések, kriptográfiai eszközök

167. Olyan nyílt adatok esetében, ahol más védelmi eszközök nem nyújtanak kellő biztonságot, kriptográfiai eszközökkel és technikákkal kell gondoskodni az adatvédelemről.

168. Az alkalmazható kriptográfiai eszközt vagy eljárást, valamint a kriptográfiai kulcsok hosszát az Informatikai Biztonságért Felelős vezető hagyja jóvá.

169. A kriptográfiai eszköz vagy a kódolási eljárás, illetve algoritmus kiválasztása előtt kockázatelemzésre van szükség. Gondoskodni kell a kulcsok kezeléséről (kiadás, megszemélyesítés, visszavonás stb.), a felelősségi köröket, felelős személyeket előre meg kell meghatározni. Az Informatikai Főosztály Információvédelmi és Rejtjel Osztálya lefolytatja a személyek oktatását és az engedélyezési eljárásokat.

170. Kriptográfiai rendszerekkel és technikákkal kell gondoskodni az adatok kódolásról, ha az adatokat illetéktelen személyek által is hozzáférhető helyen kell továbbítani vagy tárolni, valamint minden olyan esetben ahol fennáll, hogy az adatok bizalmassága sérül.

171. Az elektronikus aláírás esetében ügyelni kell a magánkulcs bizalmas kezelésére.

172. Az elektronikus aláírás kulcsa és a kódolókulcs nem lehet azonos. Az elektronikus aláírás algoritmusát, valamint az alkalmazható kulcsok hosszát az Informatikai Biztonságért Felelős vezető hagyja jóvá.

173. A le nem tagadhatóság biztosítására automatikus, a felhasználó által nem befolyásolható rendszereket kell kialakítani.

174. A kulcsmenedzsmentet minden elektronikus aláírással, kódolással rendelkező rendszerben ki kell alakítani. Ennek során a hatályos jogi szabályozást és a PKI-ra vonatkozó nemzetközi szabályozást kell figyelembe venni.

175. A kriptográfiai kulcsok fizikai, valamint speciális, illetve fokozott biztonságot igénylő esetben kódolással megvalósított logikai védelméről is gondoskodni kell. Szükség esetén a kulcs felek megosztásával kell biztosítani a kódoló kulcsok védelmét.

176. A kulcskezelési rendszer kialakításánál a következő szabványok, szempontok és módszerek egyeztetett rendszerét kell figyelembe venni:
   a) kulcsgenerálási rendszer,
   b) nyilvános kulcshitelesítési eljárások,
   c) a felhasználói kulcsok eljuttatására, valamint az átvett kulcsok aktiválására vonatkozó módszerek,
   d) kulcstárolási, illetve hozzáférési szabályok,
   e) kulcsmódosítási, aktualizálási szabályok,
   f) hamisított kulcsok kezelése,
   g) kulcsvisszavonási szabályok (a kulcsok visszavonásának és használaton kívül helyezésének módja, többek között azokban az esetekben, amikor a kulcsokat hamisítják vagy a kulcs tulajdonosa elhagyja a szervezetet),
   h) kulcsok archiválási rendje,
   i) elveszett kulcsok helyreállítási szabályai (az elveszett kulccsal kódolt állományok visszaállítása az üzletmenet-folytonossági terv része kell hogy legyen),
   j) kulcsok megsemmisítésének szabályai,
   k) kulcskezelő rendszer eseménynaplózása.

177. A kulcshamisítás kockázatának csökkentése érdekében, előzetesen meg kell határozni a kulcsok aktiválásának és visszavonásának dátumait. A kulcs élettartama függ a vélelmezett kockázat mértékétől.

178. A nyilvános kulcsokkal való esetleges visszaélések kockázatának csökkentése érdekében, csak hitelesített nyilvános kulcsok használhatók a rendszerben.

179. A kriptográfiai szolgáltatók külső szállítóival, például egy hitelesítő hatósággal kötött, a szolgáltatás mértékét meghatározó szerződéseknek szabályozniuk kell a felelősség kérdését.

180. Minden más titkosítással és rejtjelezéssel kapcsolatos feladatot, biztonsági kérdést külön szabályzatban kell rögzíteni.

34. Rendszerszintű adatállományok védelme

181. A rendszerszintű adatállományok védelmének érdekében ellenőrizni és dokumentálni kell a védendő rendszer-adatállományok elérését. A rendszer integritásának fenntartása annak a felhasználói funkciónak vagy fejlesztési csoportnak a feladata, amelyhez az alkalmazói rendszer vagy program tartozik.

182. Az informatikai rendszerek által biztosított naplózási lehetőségeket be kell kapcsolni. A rendszergazdáknak ezeket a naplókat rendszeresen ellenőrizniük kell, az ellenőrzés eredményéről rendszeresen és szükség esetén időszakosan jelentést kell tenniük.

183. A fejlesztői, a teszt- és az éles rendszereket egymástól el kell választani.

184. A BM által fejlesztett, illetve alkalmazott programok forráskönyvtárát, a programokba való illetéktelen beavatkozás lehetőségének korlátozása érdekében ellenőrzés alá kell vonni.

185. A program forráskönyvtárát lehetőség szerint az operációs rendszer állományaitól elkülönítve kell tárolni. Minden alkalmazás esetében ki kell jelölni egy olyan személyt, aki az alkalmazás forráskódjának biztonságáért felel. A program forráskönyvtáraihoz csak ezek a személyek férhetnek hozzá.

186. A program forráskönyvtárainak aktualizálását és a programforrások programozók számára való kibocsátását csak kijelölt személy végezheti, az alkalmazásért felelős vezető írásos engedélyével. A forráskönyvtár minden változásáról eseménynaplót kell vezetni.

187. A forrásprogramok korábbi verzióit archiválni kell. A program forráskönyvtárainak karbantartását és másolását a változtatásokra vonatkozó szigorú ellenőrzési eljárások alá kell vonni.

35. Informatikai biztonság a fejlesztési és a karbantartási folyamatokban

188. A fejlesztések csak az Informatikai Biztonságért Felelős vezető hozzájárulása után kezdhetők meg. A projekt- és a támogatási környezeteket szigorúan kell ellenőrizni.

189. Az alkalmazói rendszerekért felelős vezetők felelősek a projekt és a támogatás környezetének biztonságáért. Meg kell vizsgálniuk a rendszerben javasolt összes változtatást és meg kell állapítaniuk, mennyiben befolyásolják ezek a rendszer vagy működési környezete biztonságát.

190. A BM szervezeti egységénél alkalmazandó rendszerek, alkalmazások, és programok fejlesztését külön Fejlesztési Szabályokban kell meghatározni.

191. Az informatikai rendszer sérülékenységének minimalizálása érdekében a változtatásokat csak szigorú ellenőrzéseken keresztül lehet megvalósítani. A változtatás ellenőrzésének eljárását a Változásmenedzsment Szabályzatban kell szabályozni.

192. Az eljárással kapcsolatban a fejlesztési szabályokban:
   a) szabályozni kell a változtatást végrehajtó személyek körét,
   b) a szükséges módosítás érdekében az összes szoftver, információ, adatbázis és hardver azonosítását el kell végezni,
   c) a munka elkezdése előtt részletes, formalizált elfogadási eljárásra van szükség,

d) biztosítani kell, hogy a megvalósítás során a belső folyamatok ne sérüljenek,
e) a rendszerdokumentációkban a változásokat át kell vezetni, és a régi dokumentációkat archiválni kell,
f) karban kell tartani a változásmenedzsment segítségével az összes szoftverfrissítést,
g) biztosítani kell minden változtatás ellenőrzését,
h) biztosítani kell, hogy – amennyiben szükségesek – a változások az üzemi dokumentumokon is átvezetésre kerüljenek,
i) biztosítani kell, hogy a változtatások kellő időben kerüljenek megvalósításra.

193. Amennyiben a külső vagy a belső tényezők szükségessé teszik az operációs rendszer változtatását, az operációs rendszer alapértelmezett átvizsgálása után az applikációs rendszert ellenőrizni és tesztelni kell annak biztosítása érdekében, hogy a változtatás a működőképességgel és a biztonsággal ne ütközzön. Éles rendszerbe történő beillesztés előtt a változásokat az alkalmazásokkal kell tesztelni.

194. A BM munkatárs munkavégzése során csak jogtiszta szoftvereket használhat.

195. A programfejlesztés külső személyekhez való kihelyezése esetén a BM adat- és információvédelmére vonatkozó szabályok és a Fejlesztési Szabályok figyelembevételével kell eljárni. Biztosítani kell a forrásprogramot, valamint a továbbfejlesztés lehetőségét a BM részére a fejlesztőtől függetlenül is. A fejlesztés során az üzemi rendszerekhez a külső személy részére távoli hozzáférés nem engedélyezhető. Biztosítani kell annak lehetőségét, hogy az Informatikai Biztonságért Felelős vezető a fejlesztési környezetben, az informatikai biztonsági szabályok betartását ellenőrizhesse.

36. Az adatokhoz kapcsolódó egyéb intézkedések

196. A BM informatikai rendszereit használó felhasználókról adatnyilvántartást kell vezetni. A nyilvántartásnak az alábbi adatokat kell tartalmaznia:
a) felhasználó neve,
b) beosztási helye,
c) munkáltatója,
d) rendszerekhez való hozzáférési jogosultsága,
e) munkaállomásának műszaki paraméterei,
f) szolgálati adathordozójának nyilvántartási száma,
g) egyéb szolgálati információs eszközeinek listája és azok nyilvántartási számai,
h) ideiglenes engedélyeinek tárgya és lejárati ideje.

197. A BM informatikai rendszereibe adatot csak az arra jogosultsággal rendelkezők vihetnek be, dolgozhatnak fel, abból adatot csak ők szolgáltathatnak, kiadványozhatnak. Ilyen műveletre a felhasználó a vezetőjének engedélyével, adott esetben az Informatikai Főosztály vezetőjének hozzájárulásával jogosult.

198. Adatok állandó és ideiglenes tárolásának előírásairól mentési és archiválási tervben kell rendelkezni.

37. Biztonsági és üzemzavarok kezelése

199. Mérsékelni kell a biztonságot befolyásoló események és működési zavarok következményeit. Nyomon kell követni az eseményeket, biztosítani kell a mielőbbi normális üzemre való visszaállást és a tapasztalatokat feljegyzésben kell rögzíteni.

200. Mindazon biztonsági eseményeket, amelyek a folyamatos éles üzemet megzavarják, a napi feldolgozást hátráltatják, azonnal jelenteni kell a rendszer üzemeltetéséért felelős vezetőnek. A jelentés követően az üzemzavart mielőbb meg kell szüntetni.

38. A váratlan események kezelési eljárásai

201. A BM munkatársnak és a külső személyeknek ismerniük kell a szervezet működésének és az eszközök használatának biztonságát befolyásoló különböző események (biztonsági előírások megsértése, veszélyek, hiányosságok vagy működési zavarok) jelentésének eljárási szabályait. A BM-munkatársaknak írásban jelenteniük kell az észlelt eseményeket. Az események biztonságos kezeléséhez szükség van arra, hogy az eseményt követően nyomban összegyűjtsék a meglévő bizonyítékokat és felterjesszék vezetőjük felé további vizsgálatok lefolytatása céljából.

202. A biztonsági eseményre adandó gyors, hatékony és szabályos válaszadás érdekében meg kell határozni a váratlan eseményekkel kapcsolatos felelősségeket és eljárásokat, el kell készíteni az üzletmenet-folytonossági tervet.

203. A következő biztonsági események kezelésére kell egyedi eljárást kidolgozni:
   a) az informatikai rendszer hibái és a szolgáltatás megszakadása,
   b) szolgáltatás megtagadása,
   c) pontatlan és hiányos adatokból származó hibás eredmények,
   d) a bizalmasság elvesztése.

204. Az üzletmenet-folytonossági tervhez kapcsolódóan a következő eljárásokat kell alkalmazni:
   a) azonosítani és elemezni kell az események okait,
   b) terveket kell kidolgozni a nem kívánt események ismétlődésének megakadályozására,
   c) az eseményeket naplózni kell,
   d) gondoskodni kell a visszaállítás megoldásáról,
   e) a szervezetileg illetékes vezető és az Informatikai Biztonságért Felelős vezető részére jelentést kell készíteni.

205. A biztonsági események és rendszerhibák javítását a következők szerint kell végrehajtani:
   a) csak az engedéllyel és a kellő szaktudással rendelkező személyek férhetnek az „éles" rendszerekhez és azok adataihoz,
   b) az adott feladatra kijelölt vezetőnek ismernie és ellenőriznie kell minden, rendkívüli esemény során az Informatikai Főosztály vezetője által alkalmazandó/alkalmazott eljárást,
   c) minden rendkívüli esemény során az alkalmazandó/alkalmazott eljárást jegyzőkönyvben rögzíteni kell,
   d) a rendkívüli eseményeket követően az adatok sértetlenségét haladéktalanul ellenőrizni kell.

39. Biztonsági események jelentése

206. A BM munkatársa az észlelt biztonsági eseményt a szervezeti egység vezetőjének és az Informatikai Biztonságért Felelős vezetőnek jelenti, valamint mindent megtesz a szükséges bizonyítékok összegyűjtésére. A szervezeti egység vezetője jelentését és a felvett jegyzőkönyvet haladéktalanul továbbítja az Informatikai Biztonságért Felelős vezetőnek, aki az eseményt a lehető legrövidebb idő alatt kivizsgálja, és amennyiben a felelősségre vonás szükségessége fennáll, értesíti a munkáltatói jogkör gyakorlóját.

40. A rendszerek és a programok működési zavarainak kezelése

207. A BM minden szerverén és munkaállomásán folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit.

208. Rendszer-, illetve alkalmazáshiba esetén:
   a) figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket,
   b) amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett munkaállomást, számítógépet le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is (pendrive, CD-ROM, mentési médiák), melyeket az Informatikai Biztonságért Felelős vezetőnek, a BM munkatársának vizsgálat céljára át kell adni,

c) a BM hozzáférési, és egyéb adatvédelmi rendszereinek működés zavarát, a megtett intézkedéseket, haladéktalanul írásban jelenteni kell a szervezeti egység vezetőjének és az Informatikai Biztonságért Felelős vezetőnek,

d) a meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

41. Az események tapasztalatainak elemzése és értékelése

209. Az eseményeket:
   a) típus,
   b) terjedelem,
   c) általuk okozott károk, helyreállítási költségek,
   d) a feljogosítási és monitorozási rendszer működési zavara alapján értékelni kell.

210. Az elemzés alapján – szükség esetén – kezdeményezni kell a biztonsági irányelvek felülvizsgálatát, a szabályzatok korszerűsítését.

211. A biztonsággal összefüggő munkavállalói kötelességek megszegésének gyanúja esetén a felelősségi vizsgálat megindítása a munkáltatói jogkört betöltő vezető feladata.

42. Kommunikációhoz kapcsolódó védelmi intézkedések, azonosítás távoli kapcsolatnál, távdiagnosztikai portok védelme

212. A távoli felhasználók hozzáférését hitelesítéshez kell kötni. A kriptográfiai technikákra alapozott módszerek lehetővé teszik a felhasználók megbízható hitelesítését.

213. Kockázatelemzés alapján fel kell mérni a védelem szükséges mértékét, annak érdekében, hogy kiválasztható legyen a hitelesítés megfelelő módszere.

214. A távoli felhasználók hitelesítése megoldható többek között kriptográfiai technikával, gépi jelzéssel vagy kérdés/felelet protokollal. A csatlakozások forrásának ellenőrzése kiválasztott magánvonalakkal vagy hálózati felhasználói címek ellenőrzésére alkalmas eszközökkel is lehetséges.

215. A visszahívási eljárások és ellenőrző eszközök használata védelmet nyújthat a BM adatfeldolgozó eszközeihez való illetéktelen és nem kívánatos hozzáféréssel szemben. Az ilyen jellegű ellenőrzés hitelesíti azokat a felhasználókat, akik egy távoli helyről kívánnak kapcsolatot teremteni a BM hálózatával. Fontos továbbá, hogy a visszahívás folyamata garanciákat tartalmazzon arra az esetre is, hogy a BM oldalán valóban megtörténik a kapcsolat megszakítása, ellenkező esetben ugyanis a távoli felhasználó nyitva tarthatja a vonalat és szimulálhatja a visszahívás megtörténtét. Ennél a lehetőségnél gondoskodni kell a visszahívási eljárások és ellenőrző eszközök alapos vizsgálatáról is.

216. Mindegyik felhasználói igény esetében vagy a formalizált hálózati elérésekkel kapcsolatos szabályok, vagy pedig az adott esetre kidolgozott speciális elvárások alapján kell az irányelveket kidolgozni. A felhasználókkal a szolgáltatások indítása, vagy az azokkal történő kommunikáció megkezdése előtt végre kell hajtani a hitelesítési eljárást.

217. Az adott hálózati alrendszer hitelesítési mechanizmusa nem érintheti a hálózat többi alrendszerének hitelesítési rendszerét.

218. A munkavégzéshez szükséges mértékben kell a felhasználók számára a hálózati erőforrások használatát engedélyezni.

219. Megosztott erőforrások csak azonosítás után legyenek elérhetők. Munkaállomások megosztását (azok védelmének nehézsége miatt) kerülni kell.

220. Biztosítani kell a fogadó oldalon a felhasználó azonosítás utáni visszahívásának (call back) lehetőségét.

221. Csak a kellően biztonságos környezetben, megfelelő technikákkal biztosított helyeken lehet a távoli elérést biztosítani.

222. Távoli elérésre külön kezelt felhasználói csoportot kell kialakítani.

223. Egy távoli számítógéphez való automatikus csatlakozás lehetősége egy alkalmazáshoz való illetéktelen hozzáférést tehet lehetővé, ezért a számítástechnikai rendszerekhez távolról való összes csatlakozást hitelesíteni kell. Ez különösen fontos akkor, ha a csatlakozás egy olyan hálózatot használ, amely kívül esik a szervezet biztonsági rendszerének ellenőrzésén.

224. Technikailag biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásokról lehessen a rendszerekbe belépni. Egységes munkaállomásnév-használatot kell kialakítani, a hálózatban lévő munkaállomások pontos azonosítása érdekében.

225. Az informatikai üzemeltetőnek gondoskodnia kell a diagnosztikai portok hozzáférésének biztonságos ellenőrzéséről. Számos számítógép és kommunikációs rendszer rendelkezik egy tárcsázással működtethető távoli diagnosztikai eszközzel, amelyet a karbantartásért felelős műszaki szakemberek használhatnak. Kellő védelem hiányában ezek a diagnosztikai illesztőegységek az illetéktelen hozzáférés eszközeiként használhatók. A megfelelő biztonsági mechanizmussal, többek között zárral vagy eljárással gondoskodni kell arról, hogy ezekhez csak az Informatikai Biztonságért Felelős vezető engedélye és a szerződés alapján lehessen hozzáférni.

226. A távdiagnosztikai szolgáltatással rendelkező eszközök esetén a menedzselést csak azonosító és jelszó együttes használatával szabad elérni.

227. Ahol távdiagnosztikai szolgáltatás nem kerülhet alkalmazásra, ott ezt a lehetőséget kifejezetten minden esetben le kell tiltani.

43. A hálózatok biztonsági szegmentálása

228. A hálózatok biztonságának ellenőrzésére alkalmas módszerek egyike a hálózatok felosztása önálló logikai hálózati struktúrákra; ezek mindegyikét egy meghatározott biztonsági gyűrű (háló) védi. Kialakítható többek között oly módon is, hogy a két összekapcsolható hálózat között egy biztonsági kapu (pl. tűzfal) ellenőrzi a hozzáférést és a két struktúrahálózat közötti információáramlást. A konfigurációnak alkalmasnak kell lennie a két struktúrahálózat közötti forgalom szűrésére, valamint – a BM hozzáférést ellenőrző hatályos irányelveinek megfelelően – az illetéktelen hozzáférés megakadályozására.

229. A hálózatok elkülönítésének kritériumait a hozzáférés ellenőrzésére vonatkozó irányelvek és a hozzáférési igények alapján kell kialakítani; aminek során figyelembe kell venni a megfelelő hálózati útvonal-kiválasztási vagy kapuzási technológia tényleges és fajlagos költségeit és a teljesítményre gyakorolt hatását.

44. A hálózatra való csatlakozások és a hálózati útvonal kiválasztásának ellenőrzése

230. Az osztott hálózati munka, különösen a több szervezet által használt hálózat biztonsága szükségessé tesz korlátozást. Ezeket a forgalomszűrő, -ellenőrző lehetőségeket, amennyiben szükséges, a gateway és az operációs rendszeri beállításánál alkalmazni kell.

231. Korlátozó rendelkezéseket többek között a következő esetekben kell alkalmazni:
   a) elektronikus levelezés,
   b) egyirányú adatállomány mozgatása (pl. mentési rendszerek esetében),
   c) adatállomány mozgatása mindkét irányban,
   d) meghatározott időponthoz kötött hálózati hozzáférés.

232. A BM szervezetén túlterjedő hálózatoknál kötelező az útvonal-kiválasztást ellenőrző és vezérlő eszközök, módszerek alkalmazása, ahol:
   a) a rendszerdokumentációban pontosan meg kell adni az elérni kívánt eszközök címét, portszámát és egyéb, a biztonsági szűréshez szükséges adatokat,
   b) az útvonalak kialakításáért az adathálózati terület a felelős,
   c) a beállításokat minden esetben tesztelni és jegyzőkönyvezni kell.

45. A hálózati szolgáltatások biztonsága

233. A rendszer telepítése során csak azokat a hálózati szolgáltatások implementálhatóak a rendszerbe, melyekre az üzemeltetéshez feltétlenül szükség van. A rendszerüzemeltetőnek minden esetben fel kell mérnie, és minden részletre kiterjedően dokumentálnia kell az általa alkalmazott hálózati szolgáltatás egyedi egyedülálló, illetve összetett biztonsági jellemzőit. Amennyiben több hálózati szolgáltatás működik a rendszerben, úgy ezek egymásra gyakorolt hatását is elemezni kell biztonsági szempontból. A hálózati szolgáltatások biztonsági beállítása, valamint annak ellenőrzése, karbantartása a hálózatot üzemeltető szervezet feladata.

46. Az operációsrendszer-szintű hozzáférések ellenőrzése

234. Az informatikai eszközök illetéktelen elérésének megakadályozása érdekében az operációs rendszer szintjén rendelkezésre álló biztonsági lehetőségeket is fel kell használni a számítástechnikai erőforrásokhoz való hozzáférés korlátozásához. Ezeknek a következőket kell lehetővé tenniük:
   a) az engedéllyel rendelkező felhasználó személyének azonosítása és hitelesítése, szükség esetén a terminál vagy hely azonosítása,
   b) a sikeres és az eredménytelen hozzáférési kísérletek rögzítése,
   c) megfelelő hitelesítési eszközök és – jelszókezelő rendszer használata esetén – minőségi jelszavak biztosítása,
   d) adott esetben a felhasználók csatlakozási idejének korlátozása.

235. Amennyiben a kockázatok alapján ez indokolt, más hozzáférést vezérlő módszerek (pl. ujjlenyomat azonosító eszközök, chipkártya, kérdés-felelet) is alkalmazhatók.

236. A terminál automatikus azonosítása kötelező, ha fontos és indokolt, hogy egy munkát, vagy tranzakciót csak egy adott terminálról lehessen kezdeményezni.

237. A számítógéprendszerbe való bejelentkezési folyamatnak minimumra kell csökkentenie az illetéktelen hozzáférés lehetőségét. Ennek során csak a bejelentkezés eredményes befejezése után jelenhet meg a használni kívánt rendszerre vonatkozó adat, azonosító stb.

238. A bejelentkezés elfogadására vagy elvetésére csupán az összes szükséges adat megadása után kerülhet sor, sikertelenség esetén nem jelölheti meg a hibás, elrontott azonosítót, jelszót.

239. Korlátozni kell az eredménytelen bejelentkezési kísérletek számát, rögzíteni kell az eredménytelen kísérleteket, időtúllépés esetén meg kell szüntetni az adatátviteli kapcsolatot.

240. Biztonságos bejelentkezési folyamatot kell kialakítani, amelynek során:
   a) az azonosítás és hitelesítés keretében a hozzáférési jogosultságot jelszavakkal kell ellenőrizni. A jelszómenedzselést úgy kell biztosítani, hogy a jelszó ne juthasson illetéktelenek tudomására, ne legyen megkerülhető, illetve könnyen megfejthető;
   b) a felhasználók azonosítása egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas kell hogy legyen;
   c) a munkakör megváltozásakor a felhasználók hozzáférési jogosultságait felül kell vizsgálni, és ennek alapján módosítani kell;
   d) biztosítani kell a felhasználói azonosítók időszakos vagy végleges letiltásának lehetőségét;
   e) a rendszerhozzáférés szempontjából meghatározó erőforrásaihoz (pl. fájlok, tároló területek, berendezések stb.) olyan egyedi azonosítókat kell rendelni, amelyek a hozzáférési jogosultság meghatározásának alapjául szolgálnak.

241. Mindazon operációs rendszerelemeket, segédprogramokat, amelyek a munkavégzéshez nem szükségesek, nem kell telepíteni, vagy amennyiben ez elkerülhetetlen, úgy el kell távolítani azokat a rendszerből. Amennyiben ilyen rendszerelemek, segédprogramok használatára szükség van, azt jogosultságokhoz, felhasználókhoz kell kötni.

242. A kiemelt biztonsági osztályba tartozó, különösen fontos munkaállomásokat, illetve a nagy kockázatú rendszereit kiszolgáló inaktív terminálokat az inaktivitás kezdetétől számítva legfeljebb 30 perc elteltével ki kell kapcsolni, az illetéktelen személyek hozzáférésének megakadályozása érdekében. Ennek a funkciónak az inaktív időkorlát elteltével automatikus mentést kell végrehajtania, le kell törölnie a képernyőt, be kell zárnia a futó alkalmazásokat, és meg kell szüntetnie a hálózati kapcsolatokat.

243. Az alkalmazott időkorlátnak, valamint a zárolás szintjének meg kell felelnie a rendszer biztonsági osztályának.

244. Biztonsági szempontból kiemelten fontos helyeken a kapcsolatok idejére időkorlátokat kell bevezetni (pl. internetes szolgáltatások), ami az illetéktelen hozzáférés lehetőségeit és kockázatát csökkenti.

47. Alkalmazás szintű hozzáférések vezérlése

245. Az illetéktelen hozzáférés megakadályozására a felhasználói rendszereken belül biztonsági eszközöket is kell alkalmazni.

246. A programok és az adatok logikai hozzáférését minden esetben az engedéllyel rendelkező felhasználókra kell korlátozni. A felhasználói rendszernek nem szabad befolyásolnia olyan más rendszerek biztonságát, amelyekkel az adott rendszer megosztva használ különböző informatikai erőforrásokat. A felhasználói rendszerekben:
   a) a mindenkori hatályos hozzáférési irányelveknek megfelelően ellenőrizni kell az adatokhoz és a felhasználói rendszer funkcióihoz való felhasználói hozzáférést;
   b) védelmet kell nyújtani az illetéktelen hozzáféréssel szemben minden segédprogram és operációs rendszerprogram számára ott, ahol meg lehet kerülni a rendszer vagy az alkalmazás ellenőrző eszközeit.

247. Abban az esetben, amennyiben azt a kialakított rendszer sajátossága szükségessé teszi, az alkalmazás szintjén is szabályozni kell az adatelérést (pl. megfelelő menük alkalmazásával, a dokumentációhoz és a rendszerfunkciókhoz való hozzáférés szelektívvé tételével stb.).

48. A biztonsági monitoringrendszer használata

248. Az illetéktelen hozzáférések, a tiltott tevékenységek kiszűrése érdekében:
   a) figyelemmel kell kísérni a hozzáférési irányelvektől való eltéréseket, és naplózni kell a megfigyelhető eseményeket, hogy adott esetben bizonyítékul szolgáljanak a biztonsági események kivizsgálásához, és segítséget nyújtsanak a jelen szabályzat aktualizálásához,
   b) a rendszer nyomon követése tegye lehetővé az ellenőrző eszközök hatékonyságának ellenőrzését és egy, a hozzáférési irányelveknek való megfelelés hitelesítését,
   c) a biztonsági monitoringrendszert csak az arra feljogosítottak használhatják, és tevékenységüket naplózni kell.

249. A kivételes és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni és azt a hozzáférés nyomon követhetősége érdekében meg kell őrizni.

250. Az elszámoltathatóság és auditálhatóság biztosítása érdekében a naplózási rendszert úgy kell kialakítani, hogy abból utólag megállapíthatóak legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy kísérletét.

251. A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó vagy felhasználói csoport által végzett művelet egyedi regisztrálására, ennek érdekében a következő eseményeket naplózni kell:
   a) rendszerindítások, -leállítások,
   b) rendszeróra-állítások,
   c) be- és kijelentkezések,
   d) programleállások,
   e) az azonosítási és a hitelesítési mechanizmus használata,
   f) hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,
   g) azonosítóval ellátott erőforrás létrehozása vagy törlése,
   h) felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.

252. A biztonsági naplóban az egyes eseményekhez kapcsolódóan a következő adatokat is rögzíteni kell:
   a) a felhasználó azonosítása és hitelesítése esetén:
      aa) dátum,
      ab) időpont,
      ac) a felhasználó azonosítója,
      ad) az eszköz (pl. terminál) azonosítója, amelyről az azonosítási és hitelesítési művelet kezdeményezése történt,
      ae) a hozzáférési művelet eredményessége vagy sikertelensége;
   b) az olyan erőforráson kezdeményezett hozzáférési művelet esetén, amelynél a hozzáférési jogok ellenőrzése kötelező:
      ba) dátum,
      bb) időpont,
      bc) a felhasználó azonosítója,
      bd) az erőforrás azonosítója,
      be) a hozzáférési kezdeményezés típusa,
      bf) a hozzáférés eredményessége vagy sikertelensége;
   c) az olyan erőforrás létrehozása vagy törlése esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező:
      ca) dátum,
      cb) időpont,
      cc) a felhasználó azonosítója,
      cd) az erőforrás azonosítója,
      ce) a kezdeményezés típusa,
      cf) a művelet eredményessége vagy sikertelensége;
   d) a felhatalmazott felhasználók (pl. rendszeradminisztrátorok) olyan műveletei esetén, amelyek a rendszer biztonságát érintik:
      da) dátum,
      db) időpont,
      dc) a műveletet végző azonosítója,
      dd) az erőforrás azonosítója, amelyre a művelet vonatkozik,
      de) a művelet eredményessége vagy sikertelensége.

253. A naplófájlok tartalmát megadott időintervallum alapján, képernyőn és nyomtatón is meg kell tudni jeleníteni. Archiválás előtt, a naplóállományokat nem lehet megsemmisíteni, felülírni, módosítani.

254. Azoknál a rendszereknél ahol lehetőség nyílik rá, a naplóállományoknak kódoltaknak, ellenőrző összeggel ellátottaknak kell lenniük. A hibás bejelentkezési kísérletek számát rögzíteni kell.

255. A rendszergazdának nyilvántartást kell vezetni az egyes alkalmazásokhoz hozzáféréssel rendelkező felhasználói csoportokról és a jogosultságáról; illetve arról, hogy egy adott felhasználói csoport melyik alkalmazáshoz és milyen jogosultsággal férhet hozzá. Nyilván kell tartani a jelszócsere dátumát.

256. A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal ellenőrizni és archiválni kell. A biztonsági napló értékelése során meg kell határozni, hogy mely eseményeket kell jegyzőkönyvezni, melyek azok az események, amelyek szankciókat vonnak maguk után, és mik ezek a szankciók. A biztonsági naplók alapján felvett jegyzőkönyveket archiválni kell, és ennek során a megőrzési határidőket meg kell határozni. A biztonsági eseménynapló (naplófájl) és a jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől.

257. A biztonsági eseménynapló-fájlok vizsgálatához és karbantartásához a rendszernek megfelelő eszközökkel és ezek dokumentációjával kell rendelkeznie. Ezen eszközök állapotának regisztrálhatónak és dokumentálhatónak kell lennie. A rendszerben a biztonsági eseménynapló-fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.

258. Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.

259. A felhasználók által elvégzett tevékenységeket – az ellenőrizhetőség érdekében – rögzíteni, és naplózni kell a 248–258. pontok alapján.

260. Az informatikai rendszer üzemeltetéséről (a biztonsági napló mellett) üzemeltetési naplót kell vezetni, amelyet az adott informatikai rendszer üzemeltetéséért felelős szervezeti egység felelős vezetőjének és az Informatikai Biztonságért Felelős vezetőnek rendszeresen ellenőriznie kell.

261. Az informatikai rendszer üzemeltetéséről nyilvántartást (adatkérések, adatszolgáltatások, feldolgozások stb.) kell vezetni, amelyet az informatikai rendszer üzemeltetéséért felelős szervezeti egység vezetőjének rendszeresen ellenőriznie kell.

262. Kiemelt figyelmet kell fordítani az operációs rendszer és alkalmazás dokumentációjának figyelembevételével a rendszerdátum és rendszeridő beállítására.

263. A rendszerdátum és a rendszeridő beállítására kizárólag az Informatikai Biztonságért Felelős vezető által kijelölt BM-munkatársak jogosultak, az időpont beállítását jegyzőkönyvezni kell.

49. Mobil informatikai tevékenység, távmunka

264. A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot. A szükséges védelemnek összhangban kell lennie ennek a speciális munkavégzésnek a kockázataival. Mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. A mobil számítástechnikai eszközökön gondoskodni kell a kódolt adattárolásról és adatátvitelről. Távmunka, távoli hozzáférés esetén a BM érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely védelméről.

265. A mobil informatikai eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme. Ki kell alakítani a mobil informatikai eszközök megfelelő fizikai védelmét, és a kommunikációhoz védett csatornáról kell gondoskodni. Vírus- és behatolásvédelmi eszközöket kell biztosítani a mobil eszközökre. Fokozott figyelmet kell fordítani a mobil eszközökön tárolt adatok bizalmasságának védelmére. A távoli elérésre vonatkozó szabályokat a mobil informatikai eszközökre is alkalmazni kell.

266. Távmunka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, valamint a megfelelő és rendszeres ellenőrzésről.

267. A munkaállomásokon egyidejűleg modem és hálózati kártya csak az Informatikai Főosztály vezetőjének engedélyével használható.

50. Személyekhez kapcsolódó védelmi intézkedések (hozzáférés-menedzsment, irányelvek és követelmények)

268. Az adatok és folyamatok elérését a biztonsági követelmények alapján kell ellenőrizni. Ennek során meghatározásra kerültek az adatok elérésére, terjesztésére és engedélyezésére vonatkozó általános irányelvek.

269. Minden informatikai rendszer hozzáférési rendszerét a megvalósítási projekt során a biztonsági osztálynak megfelelő követelményszinten kell megtervezni. Ebben pontos tartalmat kapnak a munkakörök, az objektumok és a hozzáférési módok, melyek meghatározásához a következőket kell figyelembe venni:
   a) az egyes alkalmazások biztonsági követelményeit,
   b) az alkalmazásokra vonatkozó összes információ azonosítását,
   c) az információk terjesztésére és engedélyezésére vonatkozó irányelveket, azaz a „need to know" elvet, a biztonsági szinteket és az adatminősítés alkalmazását,
   d) különböző rendszerek és hálózatok hozzáférés-ellenőrző eszközeit és az információ minősítésére vonatkozó irányelvek közötti összhang megteremtését,
   e) az adatok és szolgáltatások elérésének védelmére vonatkozó törvényi rendelkezéseket, szabályzatokat és a szerződésekben rögzített szabályokat,
   f) azonos köztisztviselői csoportokra vonatkozó egységes irányelveket,
   g) hozzáférési jogok kezelését a kapcsolatok összes típusát felismerő osztott és hálózatba szervezett környezetben.

51. A hozzáférés ellenőrzésének szabályai

270. A szabad belátás elve szerint kialakított hozzáférés-vezérlésnél a felhasználóknak az adatállományokhoz fűződő jogosultságai egyedi elbírálás alapján személyenként vagy csoportonként kerülnek meghatározásra.

271. Az előre meghatározott munkakörök és rendszerek szerinti szerepkörök szerinti hozzáférés jogosultság vezérlés esetében az előre meghatározott felhasználói szerepkörökhöz, valamint az informatikai rendszer adatállományaihoz és erőforrásaihoz biztonsági címkéket kell hozzárendelni, amelyek tartalmát (adatcsoportok, adatvédelmi szintek, hozzáférési jogok) előre meghatározott módon kell kialakítani. Az egyes felhasználók eltérő szerepkörbe sorolhatók és megkapják a szerepkörhöz rendelt jogokat. A hozzáférés jogosságának elbírálása az adott szerepkör, illetve a hozzáférésre megcélzott adatállomány, erőforrás biztonsági címkéinek összehasonlításával történik. A szerepkör szerint meghatározott hozzáférés-jogosultság kiosztás használata a fokozott és a kiemelt biztonsági osztályokban kötelező.

272. Mindegyik informatikai rendszernél a minimálisan használandó szerepköröket, valamint az azokhoz tartozó legjellemzőbb funkciókat külön-külön kell meghatározni. A szerepkörök tartalmát a Belügyminisztérium Szervezeti és Működési Szabályzatáról szóló 7/2010. (IX. 2.) BM utasításban és más utasításokban meghatározott munkakörök határozzák meg.

273. A standard munkakörök az informatikai rendszerek védelmi rendszerterveiben nyernek konkrét értelmezést és szükség esetén további részszerepkörökre bonthatók.

274. Az informatikai rendszerrel dolgozó minden BM-munkatárs a védelmi rendszertervben konkrétan meghatározott szerepkörbe sorolandó és örökli a szerepkörre meghatározott hozzáférési jogokat.

275. A szerepköröktől történő eltérést a tervezés során a projekt vezetőjének, az üzemeltetés során az Informatikai Biztonságért Felelős vezetőnek kell meghatároznia és jóváhagyatnia az adatgazdával.

276. Új rendszerek bevezetésekor a Single Sign-On (SSO) módszer alkalmazására kell törekedni.

52. A felhasználói hozzáférés menedzsmentje

277. Az információs rendszerek illetéktelen elérésének megakadályozása, érdekében megfelelő hozzáférési rendszert kell kialakítani. Hozzáférési jogosultság csak írásban kérhető.

278. Minden szerepkör feljogosít meghatározott fizikai, illetve logikai biztonsági tartományba (pl. szerverszoba, gépterem, archiválóhelyiség, illetve adott alkalmazás, hálózati szegmens, munkahelyi állomás stb.) történő belépésre és abban az engedélyezett fizikai, illetve logikai objektumokhoz való hozzáférésre az engedélyezett hozzáférési jogokkal.

279. Eljárásokkal kell szabályozni az információs rendszerekre és szolgáltatásokra vonatkozó hozzáférési jogok kiosztásának ellenőrzését.

280. Az eljárásoknak ki kell terjedniük a felhasználói hozzáférés életciklusának minden egyes szakaszára, az új felhasználók kezdeti bejelentkezésétől az olyan felhasználók kijelentkezéséig, akik többé már nem igénylik (nem igényelhetik) az információs rendszerek és szolgáltatások elérését. Külön figyelmet érdemel az elsőbbségi hozzáférési jogok kiosztása, melyek lehetővé teszik, hogy egyes felhasználók megkerüljék a rendszer ellenőrző eszközeit.

281. Olyan be- és kijelentkezési eljárást kell működtetni, amely alapján mindegyik többfelhasználós rendszerben és szolgáltatásnál szabályozni lehet a felhasználók hozzáférését.

282. A felhasználó azonosító az informatikai rendszert használó identitásának egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas megjelenítése kell, hogy legyen az informatikai rendszerben, nem adható ki különböző felhasználók részére megegyező azonosító. Az egyedi felhasználói azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni. Biztosítani kell, hogy a felhasználó azonosítója az egyes erőforrásokhoz, folyamatokhoz és az adatokhoz való hozzáférést megfelelően szabályozza (korlátozza) és követhető, ugyanakkor a biztonsági funkciók működése során ellenőrizhető legyen a biztonsági rendszer által számára.

283. A felhasználói azonosítók képzésére központi névkonvenciós szabályzatot kell készíteni. A felhasználói azonosítók képzését a BM-en belül egy helyen kell végrehajtani.

284. A felhasználói azonosítók és jogosultságok rendszerében bekövetkezett mindennemű változást (az ellenőrizhetőség érdekében) naplózni kell.

285. Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör ellátásához szükséges minimális funkcióelérést biztosíthatják.

286. A felhasználói azonosítók nem örökérvényűek. Ennek megfelelően a következő szabályokat kell alkalmazni:
   a) a BM-munkatárs, illetve külső személyek – amennyiben munkakörük, illetve beosztásuk alapján az informatikai rendszer szolgáltatásait igénybe vehetik – munkába állásuk, az igénylőlap befogadása után kapják meg felhasználói azonosítójukat. Az utasítási jogkört gyakorló vezető a munkába lépés előtt legalább 3 munkanappal megigényli a felhasználói azonosítót a hozzáférési jogosultságok megjelölésével. Más azonosítója átmenetileg sem használható. A kapott felhasználói azonosítót haladéktalanul érvényesíteni kell;
   b) a BM-munkatársnak felhasználói azonosítóját munkaviszonya megszűnésével, a külső személyek felhasználói azonosítóját megbízatásuk lejártával, haladéktalanul le kell tiltani. A megszűnt munkaviszonyú felhasználó a rendszer szolgáltatásait nem veheti igénybe és erőforrásait nem használhatja;
   c) a jogviszonyukat huzamosabb ideig szüneteltető (pl. képviselőjelölt, gyermek szülése stb.), illetve a más okból tartósan távollévő (külföldi kiküldetés, elhúzódó gyógykezelés) BM-munkatársak felhasználói azonosítóját le kell tiltani, illetve munkába állásukkal egy időben ismét engedélyezni kell. Erről a munkatárs mindenkori vezetője írásban tájékoztatja az Informatikai Főosztályt;
   d) a kormánytisztviselők áthelyezése kapcsán felmerülő jogosultsági változásokat (megszűnő felhasználói azonosítók letiltása, vagy a jogosultságok törlése, illetve új azonosítók vagy jogosultságok létrehozása) az áthelyezéssel egy időben, haladéktalanul át kell vezetni;
   e) külső személyek, akik valamilyen okból igénybe vehetik a BM bármelyik rendszerének szolgáltatásait, csak meghatározott időre, és korlátozott lehetőségeket biztosító (pl. egy adott projekt keretein belül érvényes) felhasználói azonosítót kaphatnak, ami szerkezetileg megfelel a szervezeten belüli BM-munkatársak azonosítójának, de egyértelműen és könnyen megállapítható, hogy az adott felhasználói azonosító külső személyé;
   f) azokban a rendszerekben, amelyek regisztrálják a felhasználó utolsó bejelentkezésének időpontját, ha egy felhasználó azonosító 30 napot meghaladóan inaktívnak bizonyul (azaz a felhasználó a rendszer szolgáltatásait ez idő alatt egyszer sem vette igénybe), azonosítóját le kell tiltani és erről a BM-munkatárs munkahelyi vezetőjét értesíteni szükséges, megjelölve az érvénytelenítés okát.

53. A jogosultságok kezelése

287. Standard jogosultságok:
   a) olvasási jog (betekintés),
   b) létrehozási jog,
   c) módosítási jog,
   d) törlési jog.

288. A hozzáférés-jogosultság vezérlésére a szerepkör szerinti hozzáférés elvét kell alkalmazni, valamint a biztonsági adminisztrátori szerepkört elkülönítetten kell létrehozni.

289. A biztonsági naplóállományokat két példányban, időszakosan, és elkülönítetten tárolt, egyszer írható adathordozóra kell archiválni.

290. A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoport szinten való megkülönböztetésére és szabályozására. A hasonló szerepű személyek csoportjai munkájának támogatására hozzáférési jogosultsági csoportokat kell kialakítani.

291. A BM informatikai rendszeréhez való hozzáférési jog megadása csak a hálózatijogosultság-igénylő lap szabályos kitöltése után lehetséges. A hálózatijogosultság-igénylő lapokat az informatikai üzemeltető őrzi meg és tartja karban.

54. A felhasználói jelszavak kezelése

292. Az informatikai rendszerekben a felhasználók hitelesítésének alapvető módja a jelszó megadása.

293. A felhasználónak kötelezően alá kell írnia egy nyilatkozatot, melyben felelősséget vállal személyes jelszavainak bizalmas kezelésére.

294. A belépéskor kapott, illetve – pl. ha a felhasználó elfelejtette a jelszavát – az ideiglenes jelszó átadása csak biztonságos csatornán történhet aláírással ellátott kérelme alapján, a felhasználó előzetes – pl. személyes – azonosítása után. Az ideiglenes jelszavak megváltoztatása kötelező az első belépést követően.

295. A felhasználónak minden esetben vissza kell igazolnia új jelszavának az átvételét ellenőrizhető úton (pl. e-mail), vagy személyesen.

296. A jelszónak minden felhasználó számára szabadon megváltoztathatónak kell lennie.

297. A felhasználói jelszavakkal kapcsolatban (amennyiben az adott rendszerben erre lehetőség van) biztosítani kell a következő követelmények teljesülését:
   a) a jelszó legalább 8 karakterből álljon,
   b) a jelszót a kisbetű (a–z), nagybetű (A–Z), szám (0–9) és a jelek halmazából legalább két csoport felhasználásával kell képezni, a jelszó 12 hónapig és legalább 4 jelszóváltásig nem ismételhető,
   c) a jelszó maximális élettartama 3 hónap,
   d) a jelszó 10 sikertelen kísérlet után zárolásra kerül,
   e) a központi jelszó megadása utáni első bejelentkezéskor a kötelező jelszó cseréjét,
   f) a számítógépes rendszerekben a jelszavakat nem lehet nyílt formában tárolni. A jelszófájlokat megfelelő kódolási védelemmel kell ellátni.

298. Automatikus bejelentkezési eljárások (pl. batch-fájlok, vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót. A felhasználó azonosítók és jelszavak nem tárolhatók kódolatlan formában. Felhasználói azonosítók, jelszavak, kriptográfiai kulcsok és az ehhez tartozó jelszavak nyomtatott formában, lezárt, lepecsételt borítékban, lemezszekrényben tárolhatók. A lezárt borítékot a lezárónak alá kell írni, a lezárás dátumának feltüntetésével. Amennyiben munkahelyi felsővezetők felhasználói azonosítóit, jelszavait, illetve kódoló titkos kulcsait, vagy az ehhez tartozó jelszavakat tárolni kell, akkor azt a titkosügy-kezelésen kell lezárt, lepecsételt borítékban őrizni különösen védendő munkaállomásain mérlegelni kell chipkártyás, illetve biometrikus, vagy más azonosítás alkalmazását.

299. Biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága munkakörüknek megfelelő legyen.

300. Az Informatikai Biztonságért Felelős vezető és a Személyügyi Főosztály a rendszergazda bevonásával a jogosultságokat rendszeres időközönként felülvizsgálja. Az általános felhasználók esetében ezt évente, míg a kiemelt jogosultsággal rendelkező felhasználók esetében legalább 3 havonta kell megtenni. Rendszeresen ellenőrizni kell azt is, hogy privilegizált jogokkal csak egyedileg azonosítható felhasználók, csoportok és eszközök rendelkezhessenek.

301. Az adminisztrátori jogosultsággal rendelkező munkatársaknak az adminisztrátori tevékenységükhöz külön felhasználónevet kell kapniuk, és a napi munkavégzéshez használt felhasználónévhez és az adminisztrátori felhasználónévhez tartozó jelszó nem lehet azonos.

302. A munkakörök változását az Informatikai Főosztály felé jelezni kell, a hozzáférési jogosultságokat felül kell vizsgálni, és az új munkakörnek megfelelően módosítani kell.

55. A felhasználó feladatai

303. Meg kell akadályozni az illetéktelen felhasználói hozzáférést az informatikai rendszer erőforrásaihoz. A biztonság hatékonyságához nélkülözhetetlen az engedéllyel rendelkező felhasználók együttműködése.

304. A felhasználóknak tudomással kell bírniuk a hozzáférés hatékony ellenőrzésére alkalmas eszközök használatáról, különös tekintettel a jelszavak használatára és a felhasználó kezelésében lévő berendezések biztonságára.

305. A jelszavakat nem szabad papíron tárolni. Amennyiben ez elkerülhetetlen (pl. a kezdeti jelszó), akkor gondoskodni kell a jelszó zárt borítékban történő, biztonságos tárolásáról. Ezektől eltérően a legmagasabb jogosultságot biztosító felhasználói azonosítók esetén a jelszavakat kötelező zárt borítékban, két példányban, két különböző helyen, legalább zárható lemezszekrényben tárolni.

306. Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal módosítania szükséges.

307. A jelszó kívülálló számára ne legyen egyszerűen kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat (pl. neveket, telefonszámokat, születési dátumokat), összefüggő szövegként ne legyen olvasható.

308. Amennyiben a munkaállomásokon a hitelesítési folyamatban a beírt jelszó olvasható (az alkalmazás nem rejti el megfelelően a jelszót), az alkalmazás üzemeltetőjének figyelmeztetése alapján, a felhasználó köteles gondoskodni arról, hogy más illetéktelen személy ne láthassa meg az általa beírt jelszót.

309. A biztonságos jelszóhasználat szabályait minden felhasználóval ismertetni kell.

310. A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel.

311. Amennyiben a felhasználó multiplatformos környezetet, vagy több hitelesítést igénylő alkalmazást használ, lehetőség van a felhasználó számára egyetlen kellő hosszúságú és bonyolultságú jelszó alkalmazására az összes rendszeren. (A multiplatformos rendszerekben használatos jelszó hossza min. 12 karakter, ezen kívül vegyesen tartalmaznia kell alfabetikus és numerikus karaktereket is.) Az ilyen jelszavaknál fokozottan ügyelni kell arra, hogy ne tartalmazzanak egymást követő azonos karaktereket.

312. A felhasználóknak gondoskodniuk kell a felügyelet nélkül hagyott eszközök megbízható védelméről. A felhasználó helyiségeiben felállított és a hosszabb időre felügyelet nélkül hagyott berendezéseknél – többek között munkaállomásoknál vagy szervereknél – külön védelemre lehet szükség az illetéktelen hozzáférés megakadályozására. Mindegyik felhasználónak a harmadik személlyel meg kell ismertetnie a biztonsági követelményeket és eljárásokat.

313. Az informatikai rendszerekhez csak olyan kihelyezett terminál funkció használata engedélyezhető, melynek működése az informatikai rendszerből menedzselhető (beleértve a jogosultságok vezérlését is), továbbá abból szükség esetén kizárható. A központi védelmi funkciók és a távoli csatlakozó berendezés védelmi funkcióinak együttes megléte alapvető feltétele a távoli hozzáférési jog engedélyezésének.

314. Azokban a rendszerekben, ahol lehetőség van rá, biztosítani kell a hosszabb ideig inaktív munkaállomások rendszer által kikényszerített kijelentkezését, vagy a berendezés blokkolását (lock), például a PC-s munkaállomásoknál alkalmazni kell a jelszóval kombinált képernyővédő funkciót (a munkaállomáshoz történő visszatéréskor a képernyővédő funkció feloldása csak sikeres jelszó megadás után legyen lehetséges.).

315. A PC-s terminál használata esetén, a PC használata a nem azonosított és hitelesített felhasználók számára nem megengedett.

316. Megfelelő védelmi eszköz vagy beépített védelemmel nem rendelkező operációs rendszerek nem használhatók.

317. A napi munkavégzés befejezését követően a munkaállomások kikapcsolása kötelező.

56. A hálózati szintű hozzáférések menedzsmentje

318. A hálózatba szervezett szolgáltatások védelme érdekében szabályozni és ellenőrizni kell a belső és külső hálózatba szervezett szolgáltatások elérését annak érdekében, hogy hozzáférési jogosultsággal rendelkező felhasználók ne veszélyeztethessék a hálózatba szervezett szolgáltatások biztonságát. Ellenőrizni kell a belső és külső hálózatokban működő szolgáltatások elérését.

319. Az ellenőrzés és a menedzselés eszközei a következők:
   a) megfelelően biztonságos kapcsolatok létesítése a szervezet hálózata és más szervezetek tulajdonában levő hálózatok vagy nyilvános hálózatok között,
   b) a felhasználók és az eszközök hitelesítésének mechanizmusa,
   c) az informatikai szolgáltatások felhasználóinak menedzselése, hozzáférésük vezérlése.

320. A hálózatba szervezett szolgáltatásokhoz való nem kellően biztonságos csatlakozások hatással lehetnek a szervezet egészére. Alapvető követelmény, hogy a felhasználók közvetlenül csak azokhoz a szolgáltatásokhoz férhessenek hozzá, amelyekre engedélyük kifejezetten vonatkozik. Ennek az ellenőrzése különösen fontos az érzékeny vagy kritikus alkalmazásokhoz való hálózati csatlakozások vagy a különösen nagy kockázattartalmú helyen tevékenykedő felhasználók – többek között olyan nyilvános vagy külső területek – esetében, amelyek kívül esnek a szervezet biztonsági irányításán és ellenőrzésén.

321. A hálózatok és a hálózati szolgáltatások használata során a következő tényezőkre kell figyelni:
   a) meg kell határozni az engedélyezett hálózatok, valamint az engedélyezett hálózati szolgáltatások elérési kritériumait,
   b) az engedélyezési eljárás során meg kell határozni az engedélyezett hálózatokat és hálózati szolgáltatásokat, valamint azokat a személyeket, eszközöket, alkalmazásokat, melyek valamiképpen kapcsolatba kerülnek a hálózatokkal és a hálózati szolgáltatásokkal,
   c) menedzselési és ellenőrzési eljárásokat kell kialakítani,
   d) ezen pontoknak összhangban kell lenniük a már eddig megfogalmazott, azonosításra, hitelesítésre, hozzáférés-szabályozásra, bizalmasságmegőrzésre és az ellenőrzésre vonatkozó szabályokkal. Mindegyik igény esetében vagy a formalizált hálózati elérésekkel kapcsolatos szabályok, vagy pedig az adott esetre kidolgozott speciális elvárások alapján kell az irányelveket kidolgozni,
   e) az elektronikus úton továbbított üzenetek, állományok tekintetében az Iratkezelési Szabályzatnak megfelelően kell eljárni,
   f) a felhasználók számára a hálózati erőforrások használatát a munkájukat nem veszélyeztető mértékig korlátozni kell,
   g) az adatvesztés és sérülés elkerülése érdekében hibadetektáló és -javító eljárásokat kell alkalmazni,
   h) a hálózat elemeit rendszeresen ellenőrizni kell annak érdekében, hogy a hálózatban az erőforrásokat ne használhassák illetéktelenül.

322. A rendszergazda feladata, hogy ellenőrizze a felhasználói terminál és a szerver közötti útvonalat. A hálózatok alapvető rendeltetése, hogy biztosítsák az erőforrások megosztását és a rugalmas útvonal-kiválasztást. Ez esetenként lehetővé teheti az alkalmazások engedély nélküli elérését, vagy az informatikai eszközök engedély nélküli használatát. Egy felhasználói terminál és a felhasználó által használható számítástechnikai szolgáltatások közötti útvonalat korlátozó ellenőrző eszközök alkalmazása – azaz egy kötelező útvonal kialakítása – csökkentheti a lehetséges kockázatokat.

323. A kötelezően előírt útvonal célja, hogy a felhasználók ne választhassanak a felhasználói terminál és a felhasználó számára hozzáférhető szolgáltatások közötti – az engedélyben rögzített – útvonalon kívül eső útvonalat. Ehhez általában arra van szükség, hogy az útvonal különböző pontjain megvalósuljanak a megfelelő ellenőrző eszközök. Az elv lényege, hogy előre meghatározott választási lehetőségekkel korlátozzák a hálózat minden egyes pontján a választható útvonalak számát. Ennek lehetséges megoldásai:
   a) a hálózat aktív eszközeivel, az operációs rendszer beállításaival és az alkalmazói programokkal kell biztosítani a lehető legnagyobb fokú hálózati erőforrás-, szegmensszétválasztást, valamint a felhasználók munkájához szükséges (és csak az ahhoz szükséges) útvonalakat,
   b) kiválasztott vonalak vagy telefonszámok kijelölése,
   c) az egyes felhasználó által választható menü- és almenűopciók korlátozása,
   d) a korlátlan hálózati böngészés megakadályozása,
   e) meghatározott felhasználói rendszerek és/vagy biztonsági kapuk kötelező használatának elrendelése a külső hálózati felhasználóknál,
   f) az engedélyezett forrás és a rendeltetési hely közötti kommunikációk megelőző ellenőrzése biztonsági kapukkal, pl. tűzfalakkal,
   g) a hálózati hozzáférés korlátozása különálló logikai struktúrák (pl. zárt virtuális hálózatok) létrehozásával a szervezeten belül bizonyos felhasználói csoportok számára.

324. Az információs és informatikai eszközök, azok elhelyezési körletének élő erő által végrehajtott őrzéséről a biztonsági szabályzatban részletesen kell rendelkezni.

57. Külső személyek hozzáférése, a hozzáférés feltételei

325. A külső személyek számára is hozzáférhető informatikai rendszerek és eszközök biztonságának fenntartása érdekében a hozzáféréseket minden esetben ellenőrizni kell. Az ellenőrzésért a BM részéről felelősként, kapcsolattartóként meghatározott szervezeti egysége vezetője – amennyiben a szerződésben nem került feltüntetésre, úgy a szerződést kötő szervezet vezetője – a felelős.

326. A biztonsági kockázatokat és az ellenőrzés, valamint a felügyelet követelményeit fel kell mérni. A felmérésért a szerződést – szakmai oldalról – előkészítő személy a felelős. A külső személlyel megkötött szerződésben egyértelműen meg kell határozni az előzőekhez kapcsolódó elvárásokat.

327. Külső személyek hozzáférésénél további résztvevők közreműködésére is szükség lehet. A hozzáféréséről rendelkező szerződésekben rendelkezni kell arról, hogy más, arra jogosult közreműködők is hozzáférhetnek a különböző eszközökhöz és minden esetben rögzíteni kell a hozzáférés feltételeit.

328. A jelen szabályzat előírásainak betartása az ilyen szerződések létrejöttének, valamint az adatfeldolgozási vállalkozási szerződés megkötésének elengedhetetlen feltétele.

329. Amennyiben külső személyeknek ideiglenes hozzáférési lehetőséget kell biztosítani, azt kizárólag az engedélyeztetési eljárás után lehet megtenni. A hozzáférési engedélyt minden esetben csak a szervezeti egység (főosztály) vezetője kérheti. Az Informatikai Biztonságért Felelős vezető a biztonsági előírások figyelembevételével dönt az engedély megadásáról, a kiadott engedély másolatát átadja a hatáskörrel rendelkező osztálynak. A hozzáférést mindaddig ki kell zárni, amíg a szükséges ellenőrzést el nem végezték, illetve szerződésben nem határozták meg a hozzáférés feltételeit. A visszavonás és a lejárat időpontját minden esetben szerepeltetni kell a hozzáférési engedélyben.

330. A BM azon külső személyeknek, akik a BM számára szolgáltatásokat nyújtanak, tevékenységük végzéséhez meghatározott és engedélyezett fizikai, illetve logikai hozzáféréseket biztosít az alábbiak szerint:
   a) a hardver- és szoftvertámogató személyzet rendszerszintű vagy alacsony szintű működési felhasználással rendelkezhet,
   b) a szolgáltatók vagy más partnerek, akik az információcserében részt vesznek, az informatikai rendszerekhez vagy adatbázisrészekhez hozzáférhetnek.

331. Ahol a munkavégzés érdeke megkívánja a külső személyekkel való kapcsolattartást, a munka megkezdése előtt egyértelműen meg kell határozni a munkavégzés célját, helyét, idejét, módját, fel kell mérni az alkalmazás kockázatait, a szükséges hozzáférések típusait, a veszélyeztetett adatok, információk értékét, a külső személy által használt ellenőrzéseket. Az azonosítást különleges figyelemmel kell elvégezni.

332. A külső személyek hordozható számítógépein tárolt – a munkavégzés során megszerzett és a BM-mel kapcsolatos – adatokat a munkavégzés befejezése után visszaállíthatatlanul törölni kell, amiről a partnernek – a szerződéses kapcsolat lezárásának feltételeként – írásos nyilatkozatot kell tennie.

58. Helyszíni tevékenységet végző külső vállalkozók

333. A szerződéses vagy egyéb jogviszony alapján helyszíni tevékenységet végző külső személyek által okozott biztonsági gyengülés megelőzése érdekében:
   a) a külső személlyel kötött szerződésekben ki kell kötni a BM ellenőrzési jogosultságát,
   b) a külső személyek helyszíni tevékenységének informatikai biztonsági ellenőrzése során a munkahelyi vezetőnek együtt kell működnie az Informatikai Biztonságért Felelős vezetővel,
   c) az Informatikai Biztonságért Felelős vezetőnek – még a munka megkezdése előtt – meg kell vizsgálnia a külső személyek várható helyszíni tevékenységét.

59. Biztonsági követelmények a külső személlyel kötött szerződésekben

334. Külső személyeknek a BM informatikai rendszereihez való hozzáférése kizárólag olyan írásbeli szerződésen alapulhat, melynek az összes – informatikai biztonsággal kapcsolatos – előírása igazodik a jogszabályokhoz, a BM előírásaihoz és elfogadott szabványaihoz.

335. Külső személyek számára – a velük kötött szerződésben részletezettek szerint – az adathozzáférés, elektronikus, papíralapú, mágneses vagy bármely más típusú adathordozón történő átadás-átvétel csak az adat érzékenységéhez, kezeléséhez és az informatikai rendszer biztonsági osztályba sorolásához rendelt engedélyezési eljáráshoz kötött szabályozott és dokumentált formában történhet, az adott szerződés elválaszthatatlan mellékletét képező adatvédelmi és titoktartási nyilatkozatok tartalmának megfelelően.

336. A 335. pontban felsoroltak alól kivételt képeznek az informatikai biztonsággal kapcsolatos kötelező eseti és rendszeres adatszolgáltatások, továbbá a hatósági eljárások. Ezekről minden esetben értesíteni kell az Informatikai Biztonságért Felelős vezetőt.

60. Vállalkozási szerződés kötése, outsourcing

337. Vállalkozási szerződést csak írásban lehet kötni, és e szabályzat előírásait a szerződés megkötésénél figyelembe kell venni.

338. Vállalkozási szerződés kötése esetén az érintett informatikai rendszereket, hálózatokat, környezeteket, az azokat érintő kockázatokat, valamint az alkalmazott biztonsági eszközöket és eljárásokat, felelősségeket a két fél között létrejött szerződésben rögzíteni kell.

339. Amennyiben a vállalkozó a saját telephelyén végzi az informatikai fejlesztési tevékenységet, a BM részéről, illetve részére elektronikus hálózati kapcsolaton keresztül csak kódolva továbbíthatók a fejlesztés tárgyát képező programok és adatok a fejlesztést végzők számára. Az éles üzemű rendszerekhez a vállalkozó (ideértve a vállalkozási szerződésben nem nevesített alvállalkozókat, beszállítókat is) nem férhet hozzá.

340. Programok, adatok kizárólag átadás-átvételi jegyzőkönyv alapján adhatók át. A jegyzőkönyvnek tartalmaznia kell minden esetben, hogy a forráskód és változtatásai, valamint a hozzátartozó dokumentációk a BM tulajdonát képezik.

341. A fenti anyagokat tartalmazó adathordozókat úgy kell kezelni, hogy az adathordozók azonosíthatóak, ellenőrizhetőek legyenek, a minősítési (érzékenységi) és az azonosítási jelek vagy jelölések olvashatóan, letörölhetetlenül, levehetetlenül fel legyenek tüntetve. A vállalkozó ezekkel a jelekkel, jelölésekkel kapcsolatos kezelési szabályokat a teljes munkafolyamat során köteles betartani, ennek hiányában a teljesítést nem lehet elfogadni. Az adathordozók csak biztonsági (pl. vírus) ellenőrzések elvégzése után vehetők használatba a BM rendszerein.

342. Éles üzemi tesztek csak a BM saját fejlesztő rendszerein végezhetők.

343. A 338–342. pontokban foglalt előírások betartását, a tevékenység dokumentálását a BM részéről a felelősként, kapcsolattartóként meghatározott szervezeti egység vezetője és az Informatikai Biztonságért Felelős vezető által kijelölt személyek ellenőrzik.

344. Amennyiben a vállalkozó a saját telephelyén működő fejlesztő rendszeren dolgozik, akkor a következő főbb biztonsági szabályok az irányadók:
   a) a tevékenységet a fogadó szervezet folyamatosan felügyelje, dokumentálja és ellenőrizze e szabályzat betartását,
   b) belépési és hozzáférési jogosultságot az általános jogosultsági szinten túlmenően csak külön engedély alapján, a tevékenysége elvégzéséhez szükséges időre kapjon,
   c) távoli hozzáféréssel történő fejlesztés, az érintett szakmai vezető (főosztályvezető) kezdeményezésére, az Informatikai Biztonságért Felelős vezető előzetes írásbeli engedélyével történhet. Az erre irányuló javaslatot a fejlesztő és megrendelője köteles megindokolni,
   d) fejlesztési céllal távoli hozzáférés csak az engedélyben definiált végpontról és csak a BM ellenőrzése alatt álló védelmi rendszerrel megtámogatva történhet.

IV. Eljárási szabályok

61. Üzletmenetfolytonosság-menedzsment

345. A kritikus informatikai folyamatok védelme érdekében a meghibásodások és a rendellenességek elhárítása során:
   a) az üzletmenet folytonosságának fenntartását szolgáló eljárás a megelőző és helyreállítást vezérlő eljárások (üzletmenet-folytonossági terv, katasztrófaelhárítási terv) együttes alkalmazásával mérsékelni kell a különböző rendellenességek és a biztonsági rendszer meghibásodása által okozott fennakadásokat (ezek lehetnek többek között természeti katasztrófák, balesetek, berendezésekben keletkezett hibák, vagy szándékos cselekmények következményei stb.);
   b) elemezni kell a meghibásodások, fennakadások és üzemzavarok következményeit;
   c) az üzletmenet folytonosságának irányítása ki kell hogy terjedjen – többek között – a kockázatok azonosítására és csökkentésére alkalmas ellenőrző eszközökre, a kárt okozó események következményeinek korlátozására, valamint a lényeges tevékenységek időben történő újraindítására.

346. Az üzletmenet-folytonosság tervezését projektszerűen (projektmenedzser által kísérve) kell megvalósítani. Az üzletmenet-folytonosság biztosítási folyamatának kialakítása során a következőket kell figyelembe venni:
   a) az informatikai biztonsági kockázatok felmérése, és a bekövetkezési valószínűségek elemzése;
   b) a folytonosság megszakadásából (megszakításából) következő hatások, következmények felmérése és elemzése;
   c) az informatikai biztonságpolitikának megfelelő üzletmenet-folytonossági stratégia meghatározása;
   d) az előzőekben megfogalmazottaknak megfelelő üzletmenet-folytonossági tervek kidolgozása;
   e) az elfogadott tervek rendszeres felülvizsgálata és aktualizálása;
   f) kulcsfontosságú rendszerek kizárólag megfelelő és kipróbált katasztrófaelhárítási terv alapján működhetnek éles üzemben.

347. A megfelelő üzletmenet-folytonosság az informatikai rendszer folyamatos üzemi működésének az a szintje, amely során a kiesés kockázatának szintje a BM számára még elviselhető. Az elviselhetőség határát a támogatás szempontjából kritikus rendszerek maximált kiesési ideje határozza meg, melyet az üzletmenet-folytonossági tervben ki kell fejteni.

348. Az üzletmenet-folytonosság megfelelő szintjét a szükséges megelőző, illetve (a kiesés bekövetkezése után) visszaállító intézkedésekkel kell biztosítani, amely intézkedéseket előre meg kell tervezni (üzletmenet-folytonossági terv, katasztrófaelhárítási terv).

349. Az üzletmenetfolytonosság-tervezés eredménye az üzletmenet-folytonossági terv, amely részletesen meghatározza a kívánt üzletmenet-folytonosság fenntartásához szükséges feltételeket, szervezeti és szervezési lépéseket, valamint szabályozza a megvalósítás módját. Alapvető célja az, hogy a BM folyamatait támogató informatikai erőforrások a rendelkezésre álló üzemidőben a lehető legjobb időkihasználással és a legmagasabb funkcionalitási szinten működjenek annak érdekében, hogy a közvetlen és közvetett károk minimálisak legyenek.

350. Az üzletmenet-folytonossági tervnek részletesen meg kell határoznia a kívánt üzletmenet-folytonosság fenntartásához szükséges megelőző, helyettesítő, illetve visszaállító intézkedések megvalósításához szükséges feltételeket, szervezeti és szervezési lépéseket és a megvalósítás módját.

351. A tervezés egyik lényeges eleme a kiesési kockázatok elemzése, amelynek során mérlegelni kell az okozott kár nagyságát és az üzemzavari események, a veszélyhelyzetek bekövetkezésének gyakoriságát.

352. Az üzletmenet-folytonossági terv fő részei:
   a) helyzetfelmérés és értékelés,
      aa) projekt-előkészítő megbeszélés (feladatbehatárolás, humán- és eszközerőforrás, illetve az adminisztrációs feltételek tisztázása, projektterv megbeszélése, felhasználandó dokumentumok előzetes meghatározása),
      ab) részletes projektterv elkészítése,
      ac) projektindító megbeszélés (célok, feladatok, várható eredmények prezentációja; pontos feladat-meghatározás; projektszervezet összetétele; felhasználandó dokumentumok listája; projekt megkezdése),
      ad) előzetes helyzetfelmérő interjúterv elkészítése és véglegesítése (területek, személyek),
      ae) az interjúk megszervezése (személyek és időpontok egyeztetése), tematikák elkészítése,
      af) interjúk elkészítése és feldolgozása dokumentumokban (kritikus folyamatok és az ezeket támogató alkalmazások; a kiesések következményei, kockázatai és rangsorolása az eredményes működés szempontjából, rendelkezésre állás követelményei, potenciális üzemzavari és katasztrófaesemények palettája, tartalékolási és visszaállítási stratégiák és megoldások),
      ag) projektteam teszteli a meghatározott tartalékolási és visszaállítási megoldások megvalósíthatósági feltételeit, majd ennek alapján helyzetfelmérő és értékelő jelentést készít. A projektteam a helyzetfelmérő és értékelő jelentését a szervezet vezetőjének átadja, aki a jelentést ellenőrzi és elfogadja;
   b) az üzletmenet-folytonossági terv kidolgozása,
   c) oktatás, tréning és tesztelés: célja az üzletmenet-folytonosság jelentőségének tudatosítása, az üzletmenetfolytonosság-tervezés alapismereteinek átadása, a megelőzési és visszaállítási tervben foglaltak megismerése és elsajátítása.

353. Az üzletmenet-folytonossági terv kidolgozásának részei:

a) megelőzési terv és intézkedés: tartalmazza mindazon szabályzatokat, dokumentumokat és intézkedéseket, amelyek az informatikai rendszer folytonos üzemét valamilyen módon veszélyeztető tényezőkkel kapcsolatosak. A megelőzési terv a következőkre terjed ki:

aa) az informatikai rendszer megbízható üzemeltetésére és az üzemeltetésre vonatkozó intézkedésekre,

ab) az informatikai rendszer kritikus elemeinek üzemi és katasztrófa tartalékmegoldásaira és ezek üzemkészségét biztosító intézkedésekre,

ac) az informatikai rendszer üzemét biztosító környezeti rendszerek karbantartási, illetve az ezekkel kapcsolatos biztonsági intézkedésekre,

ad) az üzemeltetési dokumentáció és dokumentumok rendszerezett és biztonságos tárolására,

ae) az adathordozók rendszerezett és biztonságos tárolására,

af) az üzemeltető, a karbantartó, és a kárelhárító személyzet rendelkezésre állását és bevethetőségét biztosító intézkedésekre,

ag) a külső szervizre, a tartalékképzési megoldásokra vonatkozó, és a biztosítási szerződésekkel kapcsolatos intézkedésekre,

ah) mentési tervre, amely meghatározza a mentési rendszer generációit és hierarchiáját,

ai) az üzemelő rendszer konfigurációjában, az üzemelő szoftverben megvalósítandó változások szabályozott kivitelezésére, valamint a szoftverfejlesztések elkülönített kivitelezésére és a fejlesztett szoftverek rendszerbe történő integrálására vonatkozó legfontosabb intézkedésekre,

aj) vírusvédelmi és vírusmenedzsment-intézkedésekre, figyelembe véve a szervezetnél hatályos vírusvédelmi szabályzatot,

ak) a megelőzésben fontos szerepet játszik az alkalmazói rendszerek használatára történő rendszeres oktatás, illetve az informatikai biztonság olyan szintű oktatása, amely kiterjed az informatikai rendszerekben kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának megőrzése érdekében betartandó szabályokra és az érvényesítendő védelmi intézkedésekre,

al) tesztelési és tréningtervre, amely meghatározza a tesztelés formáit. Két formája javasolt: auditálás jellegű check-listás teszt, amelyet egy előre elkészített ellenőrzési lista alapján független belső vagy külső auditorok végeznek el, illetve valós üzemzavar- vagy katasztrófaesemények szimulációja.

b) visszaállítási terv: célja az, hogy az üzemzavar- vagy katasztrófaesemények bekövetkezése esetén az esemény azonosítása, a szükséges emberi és eszközerőforrások haladéktalan mozgósítása, és a visszaállítás a lehető leggyorsabban és szervezetten történjen meg a tervben meghatározott utasítások szerint. A visszaállítási terv a következőket tartalmazza:

ba) a visszaállítási terv célját és használatát,

bb) az üzemzavar- és a katasztrófaesemények meghatározását,

bc) az események bekövetkezési és kezelési időszakait,

bd) az eseménykezelő team összetételét, feladatait és hatáskörét,

be) visszaállítási intézkedéseket a következő lépésekre: azonnali válasz (riadóterv), futtató környezet helyreállítása, funkcionális helyreállítás, üzemeltetési szintű helyreállítás, áttelepülés (katasztrófa esetén), normalizáció az áttelepülés után.

354. Az intézkedések átfogják a központi erőforrások, azok fizikai és személyi környezetét, a végponti munkaállomások és a kommunikációs rendszer területeit.

355. Az előzetes intézkedési tervnek tartalmaznia kell mindazon feltételek biztosítására vonatkozó intézkedéseket, amelyek megléte nélkül az üzletmenet-folytonossági terv nem működőképes és a következő projektfázisban elvégzendő üzletmenet-folytonossági terv tesztje és tréningje nem valósítható meg.

356. Az üzletmenet-folytonossági terv tesztelése és tréningje akkor válik elindíthatóvá, ha a szervezet által az üzletmenet-folytonossági terv készítési fázisa végén elfogadott intézkedési tervben foglaltak olyan szinten megvalósultak, hogy az üzletmenet-folytonossági terv tesztje és tréningje meghatározott üzemzavar és katasztrófaeseményre kivitelezhető.

357. Az üzletmenet-folytonossági terv tesztje szimulált esemény bekövetkezésével és a terv szerinti visszaállítással kerül megvalósításra, amelynek keretében az eseménykezelő team, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv utasításainak végrehajtását.

358. A katasztrófaelhárítási terv globális helyettesítő megoldásokat ad megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett katasztrófa esemény után az informatikai rendszer funkcionalitása degradált vagy eredeti állapotába visszaállítható.

359. A katasztrófaelhárítás-tervezés célja a kiesési idő, a rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt a kockázatokkal arányosan lehessen megvalósítani. A vészhelyzetekből eredő károk megelőzésének, mérséklésének alapvető követelménye a részletes terv (megelőzési és visszaállítási terv) elkészítése, tesztelése és a végrehajtás rendszeres gyakorlása. Veszélyhelyzetek:
a) elemi kár,
b) áramszünet,
c) rendszerleállás,
d) szolgáltatásszünetelés,
e) adatsérülés,
f) adatvesztés.

360. A katasztrófaelhárítási terv eljárások vagy tevékenység lépések sorozata annak biztosítására, hogy a BM információfeldolgozó képességeit – a szükséges aktuális adatokkal – a bekövetkezett katasztrófa után elfogadhatóan rövid időn belül helyre lehessen állítani. A katasztrófaelhárítási terv meghatározza a következőket:
a) a rendelkezésre állási követelmények megadása,
b) a katasztrófa- vagy vészhelyzetesemények definíciója,
c) a korlátozott informatikai üzem fogalma (visszaesési fokozatok) és a hozzájuk tartozó funkcionalitási szintek,
d) javaslat a felelősségek szabályozására veszély vagy katasztrófa esetén,
e) a riadóterv vázlata,
f) kiválasztott esetekre konkrét intézkedési terv, különösen a következő területen:
fa) a szükségüzem esetére a minimális hardver- és szoftverkonfiguráció rögzítése (beleértve az adatokat is),
fb) a szükségüzem esetére – amennyiben az lehetséges – manuális póteljárás rögzítése,
fc) szükség esetén backup-rendszer (pl. saját vagy külső tartalék központ, igénybevétele),
fd) adatrekonstrukciós eljárások bevezetése,
fe) az újraalkalmazhatóságot lehetővé tevő intézkedések;
g) az olyan informatikai rendszerek védelme, amelyeknek állandóan elérhetőeknek kell lenniük (pl. redundancia intézkedésekkel és a hibákat toleráló hardverekkel és szoftverekkel),
h) az adatbiztosítási intézkedések megvalósítási szabályainak összeállítása (pl. háromgenerációs elv),
i) az üzemi szempontból szükséges adatok biztonsági kópiáinak elkészítése meghatározott időszakonként,
j) a biztonsági másolatoknak más biztos helyen (a munkaterületen kívüli) raktározása,
k) az installált rendszerszoftverek és a fontosabb alkalmazói szoftverek referenciamásolatainak biztonságos raktározása,
l) a fontosabb dokumentációk megkettőzése és raktározása,
m) a megvalósított adatbiztosítás ellenőrizhető dokumentációja,
n) visszaállítási terv, amely magában foglalja az informatikai alkalmazások prioritásainak kijelölését és a célkitűzések megállapítása (pl. az X alkalmazás újraindítása Y napon belül),
o) a beszállítói (szolgáltatói) szerződésekre vonatkozó – katasztrófaesemények bekövetkezése esetében érvényes – követelmények meghatározása (annak érdekében, hogy katasztrófahelyzetben is biztosítani lehessen a rendelkezésre állást),
p) javasolt biztosítások katasztrófák, káresemények esetére,
q) a terv készítésének, felülvizsgálatának, tesztelésének időpontja.

361. A katasztrófaelhárítási terv részei:
   a) a katasztrófaelhárítási terv definíciója;
   b) a mentési (megelőzési) terv: azon lépések sorozata, amelyeket azért hajtanak végre (a normál üzem során), hogy lehetővé tegyék a szervezet hatékony reagálását a katasztrófára. A mentési terv elmentett eszközöket (adatokat, szoftvereket) biztosít a helyreállításhoz. Így például a számítógép, a háttértárak tükrözése és az optikai tárolók használata sokkal könnyebbé teheti adatbázisok, illetve nagy tömegű papíralapú dokumentumok helyreállítását;
   c) a helyreállítási és újraindítási terv: a helyreállítási terv olyan eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy helyreállítsák az informatikai rendszert a tartalék központban vagy az adatfeldolgozó központot. A helyreállítási terv szakaszai:
      ca) azonnali reakció: válasz a katasztrófahelyzetre, a veszteségek számbavétele, a megfelelő emberek értesítése és a katasztrófaállapot megállapítása;
      cb) környezeti helyreállítás: az adatfeldolgozó rendszer (operációs rendszer, programtermékek és a távközlési hálózat) helyreállítása;
      cc) funkcionális helyreállítás: az informatikai rendszer alkalmazásainak és adatainak helyreállítása, az adatok szinkronizálása a tranzakcionaplóval. Az elvesztett vagy késleltetett tranzakciók ismételt bevitele. Az üzemeltetők, a rendszeradminisztrátorok, az alkalmazók és a végfelhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet;
      cd) áttelepülés: az informatikai rendszer kiépítése és telepítése a hidegtartalék létesítményben (ha a melegtartalék-létesítmények használata időben korlátozott);
      ce) normalizáció: az új állandó informatikai rendszer kiépítése és arra az üzemelő rendszer áttelepítése;
   d) tesztelési terv: azokat a tevékenységeket tartalmazza, amelyek ellenőrzik és biztosítják a katasztrófaelhárítási terv működőképességét;
   e) a karbantartási (üzemben tartási) terv: a szervezet változása esetén a karbantartási tervet kell felhasználni a katasztrófaelhárítási terv aktuális állapotban tartására;
   f) az érintett személyek elérési adatai.

362. Intézkedni kell:
   a) a kár megelőzésére és a károk minimalizálására a jelen szabályzatban foglaltak alapján (pl. belső vagy külső háttér-, illetve tartalékszámítógép-kapacitás előkészítése szükségüzem esetére az elégséges hardver- és szoftverkonfiguráció rögzítésével),
   b) a katasztrófák, veszélyhelyzetek bekövetkezésekor,
   c) szolgáltatás visszaállítás,
   d) a rendszer (folytonosságának) visszaállítására a katasztrófákat és a káreseményeket követően,
   e) a veszélyhelyzetek és a katasztrófák esetszimulálására, begyakorlásra, intézkedések modellezésére, illetőleg kipróbálására.

363. A tervek tesztelését egy szimulált esemény bekövetkezésével és a terv szerinti visszaállítással kell megvalósítani. Ennek keretében az eseménykezelő szervezet, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv utasításainak végrehajtását.

364. A teszt értékelése során az üzletmenet folytonosságát biztosító terveket módosítani, aktualizálni kell, és gondoskodni kell azok egymáshoz való illesztéséről. A terveket a folytonosan változó helyzethez, körülményekhez (személyzet, stratégia, infrastruktúra), követelményekhez (szabályok, kockázatok) is hozzá kell igazítani.