A Társadalmi Esélyteremtési Főigazgatóság
15./2020(..V..15..) TEF szabályzata
az informatikai biztonságról

A Társadalmi Esélyteremtési Főigazgatóság Szervezeti és Működési Szabályzatának 4.§ (7) bekezdés c) pontjában foglalt feladatkörömben eljárva az informatikai biztonságról szóló szabályokat a következők szerint állapítom meg:

1. Általános rendelkezések

1. Jelen dokumentum a Társadalmi Esélyteremtési Főigazgatóság (a továbbiakban: Főigazgatóság) informatikai biztonsági szabályzata (a továbbiakban: szabályzat).
2. A szabályzat alapvető célja, hogy a Főigazgatóság az általa használt, üzemeltetett vagy felügyelt informatikai rendszerek működtetése, üzemeltetése során biztosítsa az adatvédelem elveinek, az információbiztonság követelményeinek érvényesülését, valamint, hogy a Főigazgatóság az informatikai szolgáltatás területén biztosítsa:
   a) az informatikára vonatkozó törvényi előírások érvényesítését,
   b) a folyamatos informatikai üzembiztonság fenntartását, és
   c) az informatikai vagyon védelmét és megőrzését.
3. Jelen szabályzat hatálya kiterjed a Főigazgatóság tulajdonában, kezelésében lévő valamennyi informatikai rendszerre és azok elemeire, az ott használt alkalmazásokra és adatbázisokra, valamint az általuk keletkeztetett, feldolgozott, tárolt, továbbított valamennyi adatra és információra (függetlenül azok megjelenési formájától), minden eszköz műszaki-, valamint az informatikai folyamatok dokumentációjára.
4. Jelen szabályzat hatálya a Főigazgatóság valamennyi szervezeti egységére, a Főigazgatósággal kormányzati szolgálati jogviszonyban álló kormánytisztviselőre, munkaviszonyban álló munkavállalóra, továbbá megbízási jogviszonyban álló személyekre (a továbbiakban: felhasználó) terjed ki.
5. Jelen szabályzat alkalmazásában:
5.1. Adat: az információ hordozója, megjelenési formája, értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) jelsorozat, olyan jelsorozat, amelyből információ nyerhető ki.
5.2. Adatállomány: adathordozón tárolt, jelképes névvel ellátott adathalmaz.
5.3. Adatbázis: a megfelelő kezelőszoftverrel rendszerbe szervezett, egy vagy több adatállomány.
5.4. Adatbázis-motor: adatbázis-kezelő programok közös, szabvány szerint működő, az adatbázisok elemeit kezelő, hozzáférést, adatfeldolgozást, keresést és egyéb funkciókat kiszolgáló alapmodulja. Az adatbázis-motor az adatbázis kezelő programok vázaként működik, ezek moduljait is vezérli, működésüket alapszabályok szerint definiálja, a kiegészítő funkciókat, illesztéseket szabályozza.
5.5. Adathalmaz: valamilyen feldolgozás részére rendelkezésre álló adatok összessége.
5.6. Adatátvitel: adatok szállítása összeköttetéseken, összekötő utakon, informatikai eszközök között.
5.7. Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
5.8. Adatbiztosítás: szélesebb értelemben azon intézkedések összessége, amelyek célja az adatbiztonság szavatolása. Szűkebb értelemben az az intézkedés, amelynek megvalósítása során az adatok biztonsági okokból (rendelkezésre állás és sértetlenség) rendszeresen mentésre kerülnek.

5.9. Adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.
5.10. Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége. Így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérlenyomat, DNS-minta, íriszkép) rögzítése.
5.11. Adatvédelem: az adatok jogosulatlan megszerzésének, illetve manipulálásának megakadályozására irányuló intézkedések összessége.
5.12. Alkalmazói program (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja.
5.13. Bejelentkezés: az informatikai rendszer és egy felhasználó között olyan kapcsolat kezdeményezése az utóbbi által, amelynek során számára az informatikai rendszer funkcióinak használata lehetővé válik, valamint a felhasználó egyértelműen azonosítható lesz.
5.14. Bizalmas információ: az információ létezését vagy tartalmát csak az erre feljogosított személyek, egy meghatározott biztonsági szinten érhetik el.
5.15. Bizonyítható azonosítás: a hozzáférési folyamat jogosultság ellenőrzése során, olyan azonosítási eljárás, amelynek segítségével kétséget kizáróan, utólag is bizonyítható a felhasználó, illetve a szolgáltatást igénybevevő kiléte.
5.16. Biztonsági esemény („incidens"): olyan esemény, amely bármelyik biztonsági alapelvet (bizalmasság, sértetlenség, rendelkezésre állás) megsértette, és ez által az adatvédelem sérülése bizonyított, vagy nagy bizonyossággal vélelmezhető.
5.17. Elektronikus levelező rendszer: olyan informatikai rendszer, amely az elektronikus levelek (e-mail) küldésére és fogadására szolgál. Alapelemei: felhasználói postafiók, technikai fiók, terjesztési lista, nyilvános naptár, jogosultságok (betekintési, szerkesztési, meghatalmazotti levélküldési, tulajdonosi, adott email címről történő levélküldési jog). Saját üzemeltetésű, vagy külső szolgáltatótól átvett szolgáltatás keretében vehető igénybe.
5.18. Elektronikus levelező rendszer – felhasználói postafiók: a Főigazgatóság által a felhasználó – munkavégzés – céljából rendelkezésére bocsátott elektronikus postafiók, amelyhez a felhasználó hozzáféréssel rendelkezik és a munkakörében meghatározott feladatok elvégzéséhez, a Főigazgatóság és a kirendeltségek munkatársaival, valamint külső személyekkel történő kapcsolattartásra használja. A felhasználói fiók meghatározottan egyetlen személyhez kötődik. A postafiók főbb elemei: beérkezett üzenetek mappa és almappái, elküldött üzenetek mappa és almappái, személyes naptár, magáncélú elektronikus levelek tárolására létrehozott, kötött elnevezésű mappa.
5.19. Elektronikus levelező rendszer – technikai fiók: olyan elektronikus postafiók, amely jellemzően több felhasználó által használt (a felhasználók előre definiált jogosultsági szinttel férnek hozzá). A technikai fiók egy megadott struktúrájú megnevezéssel rendelkezik.
5.20. Elektronikus levelező rendszer – nyilvános naptár: az elektronikus levelező rendszer speciális objektuma, amely a személyes naptárral megegyező feladatot lát el. A naptárhoz egy adott felhasználó előre definiált hozzáféréssel (betekintési joggal, szerkesztési joggal, nincs jogosultsága) láthatja az objektum tartalmát (naptárbejegyzéseket).
5.21. Elektronikus levelező rendszer – betekintési jogosultság: az elektronikus levelező rendszerhez tartozó alap jogosultságszint, amelyet felhasználói postafiók mappájához, technikai postafiókhoz, valamint nyilvános naptárhoz rendelhetünk. Ezzel a jogosultsággal a felhasználó a

mappák tartalmába betekintést nyer, elemein változtatni nem tud, az elemek áthelyezése, törlése, új almappa létrehozása nem megengedett.

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

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

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

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

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

5.27. Felhasználó: a 4. pontban megjelölt személy, aki a Főigazgatóság által biztosított, üzemeltetett informatikai rendszereket használja a feladatai megoldásához.

5.28. Hardver: az informatikai rendszer fizikai elemei.

5.29. Hálózat: két vagy több számítógép, vagy általánosságban informatikai rendszerek összekapcsolása, amely a komponensei közötti adatcserét teszi lehetővé.

5.30. Helpdesk rendszer: olyan információs rendszer, amely a felhasználók hibabejelentéseinek és egyéb informatikát érintő bejelentéseinek kezelését és az intézkedések dokumentálását, nyomon követését teszi lehetővé.

5.31. Hozzáférés: olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.

5.32. Informatika: olyan tudomány, amely elméletet, szemléletet és módszertant ad a számítógépes információfeldolgozás tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

5.33. Informatikai biztonság: az informatikai rendszer olyan állapota, amelyben az adatokhoz minden felhasználó kizárólag jogosultsága mértékében képes hozzáférni. Az adatok egyéb (nem szabályozott) módon nem változnak és hitelességük megállapítható. Az adatoknak és a rendszernek a használatra jogosult felhasználók részére történő rendelkezésre állása is szükséges feltétele a biztonságnak.

5.34. Informatikai eszközök: minden olyan hardver és szoftver elem, mely az informatikai és számítástechnikai rendszerek működésében részt vesz.

5.35. Informatikai rendszer: a hardverek és szoftverek olyan kombinációjából álló rendszer, amelyet az adat- illetve információkezelés különböző feladatainak és folyamatainak teljesítésére alkalmaznak.
5.36. Informatikai támadás: minden olyan hardver vagy szoftver elem működését befolyásoló tényező, amely szándékosan akadályozza azok működését vagy kárt tesz azokban.
5.37. Intranet: olyan internetes technológiákon alapuló informatikai rendszer, amelyet kizárólag a központi szerv és a kirendeltségek felhasználói használatára alakítottak ki. Bármilyen tartalom csak a felhasználó hozzáférését biztosító adatok (felhasználónév és jelszó) megadása után válik elérhetővé.
5.38. Illetéktelen személy: olyan személy, aki az adat megismerésére nem jogosult.
5.39. Központi kommunikációs rendszer: olyan információs rendszer, amely alkalmas azonnali (prompt) üzenetek váltására a központi szerv és a kirendeltségek felhasználói között.
5.40. Külső Személy: A főigazgatósággal szerződéses kapcsolatban álló személy vagy szervezet, aki vagy amely a Főigazgatóság rendszerével kapcsolatba kerülhet.
5.41. LAN (Local Area Network): helyi számítógépes hálózat.
5.42. Működőképesség: a rendszernek és elemeinek, az elvárt és igényelt üzemelési állapotban való fennmaradása.
5.43. Mentés: informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra másolatokat készítenek.
5.44. Pótlólagos szoftver: olyan kiegészítő szoftver, amelyet a védelem erősítésének érdekében alkalmaznak.
5.45. Program: eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.
5.46. Rendelkezésre állás: az a tényleges állapot, amikor információk vagy adatok elérhetősége és a rendszer működőképessége az arra jogosultak számára sem átmenetileg, sem pedig tartósan nincs akadályozva.
5.47. Rendszerprogram (rendszerszoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassák és az alkalmazói programokat működtessék. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.
5.48. Sértetlenség (integritás): az információ sértetlensége alatt azt a fogalmat értjük, hogy az információkat, adatokat, és a programokat csak az arra jogosultak változtathatják meg és azok más módon nem módosulhatnak.
5.49. SPAM: kéretlen üzleti, politikai vagy vallási célú e-mail, fax vagy SMS, legtöbbször kereskedelmi célú és nagy mennyiségben kiküldött üzenet.
5.50. Szoftver: valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.
5.51. Tartomány: a hálózaton lévő szerverek és más számítógépek logikai csoportja, amelyek egy közös biztonsági és bejelentkezési nyilvántartó rendszert használnak. A tartományba nem csak a helyi hálózaton, hanem távoli helyszíneken lévő számítógépek is beléptethetőek.
5.52. Tűzfal (firewall): a belső hálózatot a külső hálózattól védő szoftver vagy hardver eszköz. Szabályozza a két oldal közötti információáramlást, biztosítja, hogy az alkalmazások csak a számukra engedélyezett erőforrásokat érhessék el.
5.53. Védelmi mechanizmusok: olyan védelmi intézkedések, amelyeket biztonsági szabványok határoznak meg, a hardver- és szoftvergyártó cégek pedig termékeik előállítása során építik be és szolgáltatják a felhasználók részére.
5.54. Vírus: olyan programtörzs, amely önállóan vagy a felhasználói programba épülve annak normál működését akadályozza. A felhasználói program alkalmazása során „trójai faló"-ként működhet, azaz a felhasználó tudta nélkül hajt végre illegális feladatokat, közben „megfertőzhet" az informatikai rendszerben lévő más rendszer- vagy felhasználói programot is, esetleg

megsokszorozva önmagát (lehet mutáns is). A logikai bomba a vírusnak olyan része, amelyik adott feltétel teljesüléséhez (pl. időhöz, esemény bekövetkezéséhez, logikai változó adott értékéhez) kötött módon aktivizálódik.
5.55. WAN (Wide Area Network): nagy távolságú számítógép-hálózat.

2. A szabályzat kapcsolódásai, végrehajtása és felülvizsgálata

6. Jelen szabályzatot a mindenkor hatályos jogszabályokkal és a Főigazgatóság belső szabályzataival összhangban kell alkalmazni.
7. A szabályzat kidolgozása, ellenőrzése és karbantartatása a Humánerőforrás-gazdálkodási és Informatikai Főosztály Informatikai Osztályának (a továbbiakban: Informatikai Osztály), azon belül az elektronikus információs rendszerek biztonságáért felelős személy (a továbbiakban: informatikai biztonsági referens) feladata és hatásköre.
8. Jelen szabályzatban foglalt szabályok végrehajtását vizsgálatai során a Belső Ellenőrzési Osztály is ellenőrizheti.
9. A Főigazgatóság jelen szabályzatának hatálya alá vont informatikai eszközök és rendszerek kezelése, a benne foglalt szabályok érvényesítése, betartatása az Informatikai Osztály feladata. Jelen szabályzat betartatásában az Informatikai Osztály minden munkatársának munkaköri kötelessége részt venni napi munkája során.
10. Jelen szabályzat betartásának ellenőrzése az Informatikai Osztály munkatársainak kötelessége.
11. Jelen szabályzat betartása és betartatása a Főigazgatóság minden felhasználójának és szervezeti egység vezetőjének munkaköri kötelessége.
12. Jelen szabályzat hatálya alá tartozó valamennyi felhasználónak ismernie kell azokat a követelményeket és feladatokat, amelyeket számára a szabályzat meghatároz.
13. A szervezeti egységek vezetői kötelesek gondoskodni arról, hogy a Főigazgatóság felhasználói a megfelelő ismereteket megkapják.
14. Jelen szabályzat hatálya alá tartozó valamennyi felhasználó köteles az Informatikai Osztály vezetőjét minden olyan tényről, eseményről közvetlenül vagy a szervezeti egységének vezetőjén keresztül közvetve értesíteni, ami a szabályzat rendelkezéseinek végrehajtását akadályozza vagy azokkal ellentétes.
15. Jelen szabályzat végrehajtásának eszközei:
    a) az egyes informatikai rendszerek oly módon történő kialakítása, beállítása, hogy az informatikai rendszer kikényszerítse a szabályzat rendelkezéseinek betartását,
    b) a szabályzat kötelező betartatása,
    c) a szabályzat betartását célzó rendszeres és időszaki ellenőrzések átfogó vagy célzott jelleggel (tételes vagy szúrópróbaszerű ellenőrzési módszerekkel),
    d) a hálózat és a szerverek rendszeres monitorozása, a naplók és nyilvántartások pontos és napra kész vezetése, azok rendszeres ellenőrzése,
    e) a szervezeti egység vezetőjének tájékoztatása a szervezeti egységet érintő ellenőrzési tapasztalatokról, fegyelmi vétségekről vagy biztonsági eseményekről, az elkészített jegyzőkönyvek, jelentések, feljegyzések másolatának megküldése útján,
    f) a szabályzat rendszeres megsértőivel szemben a jelen szabályzatba foglalt ismeretek oktatásán való kötelező részvétel elrendelése és az ismeretek számonkérése évente (az informatikai biztonsági referens által összeállított és kiértékelt kérdőíven), valamint
    g) a szabályzat rendszeres megsértőivel szembeni fegyelmi szankciók alkalmazása.
16. Jelen szabályzatot az Informatikai Osztály köteles felülvizsgálni és szükség esetén módosítani, az alábbi esetekben:

a) minden olyan szervezeti változás esetén, amely a szabályzatban hivatkozott szervezeti egységek bármelyikének megszűnésével vagy jelentős átalakulásával jár,
b) súlyos informatikai biztonsági események („incidensek") után, az esemény tanulságait figyelembe véve, és
c) minden olyan jogszabályváltozás esetén, amelyek jelen szabályzatban foglaltak érvényességét módosíthatják.

17. Az Informatikai Osztály köteles legalább évente egy alkalommal megfelelőségi vizsgálatot végezni, és amennyiben szükséges, a jelen szabályzatot módosítani. A megfelelőségi vizsgálat során különösen az alábbiakat kell vizsgálni:
a) jelen szabályzat betartásával kapcsolatos ellenőrzések eredményét,
b) a „Helpdesk" rendszer működését, a felmerülő problémák és hibák jellegét és tanulságait, valamint
c) az időközben felmerülő informatikai és adatvédelmi eseményeket és az ezekkel összefüggő biztonsági vonzatokat.

3. Informatikai biztonsági feladat-, felelősségi és kompetencia körök

18. A főigazgató:
a) gondoskodik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: 2013. évi L. törvény) végrehajtásáról,
b) kinevezi az elektronikus információs rendszer biztonságáért felelős személyt,
c) jóváhagyja a rendszerek biztonsági osztályba sorolását és az ahhoz kapcsolódó szabályzatokat, stratégiákat,
d) hatáskörében részt vesz a fontosabb informatikai döntésekben, különösen informatikai beruházások, fejlesztések engedélyezésében, és az informatikai biztonságot meghatározó, befolyásoló területek, tevékenységek összehangolásában. Az e pontban részletezett hatáskörét a főigazgató jogosult olyan vezető beosztású alkalmazottra delegálni, aki részt vett a Nemzeti Közszolgálati Egyetem által indított „az elektronikus információs rendszerek védelméért felelős vezető számára" képzésen (valamint a képzési formához tartozó éves továbbképzéseken).

19. Az Informatikai Osztály vezetője:
a) gondoskodik a 2013. évi L. törvény végrehajtásához szükséges feladatok ellátásáról,
b) meghozza a Főigazgatóság informatikai rendszerével kapcsolatos szakmai döntéseket,
c) megteszi a külső szervezetek számára a szakmai nyilatkozatokat és tájékoztatásokat,
d) kijelöli az általános, vagy feladathoz kötött helyettesét,
e) irányítja az Informatikai Osztály dolgozóit,
f) kijelöli és meghatározza az informatikusok általános és speciális feladatait,
g) meghatározza az informatikai felelősségi köröket,
h) meghatározza az informatikai oktatási irányokat és gondoskodik azok megvalósításáról,
i) gondoskodik a Főigazgatóság informatikai stratégiájának megalkotásáról, valamint
j) gondoskodik a Főigazgatóság informatikai eszköz- és adatvagyonának védelméről az eljárások és folyamatok szabályozása útján.

20. Az Informatikai Osztály informatikusa:
a) ellátja az Informatikai Osztály vezetője által meghatározott informatikai munkaterületeket, feladatokat és célfeladatokat,
b) ellátja a Főigazgatóság meghatározott telephelyeinek informatikai feladatait,
c) elvégzi az Informatikai Osztály vezetője által a részére kijelölt egyéb feladatokat,

d) munkakapcsolatot tart a Főigazgatóság szervezeti egységeinek dolgozóival, és vezetőivel, valamint az üzemeltetési feladatokat ellátó külső szervezetek munkatársaival,
e) a Főigazgatóság érdekében érvényesíti az informatikai előírásokat, valamint
f) eljár és intézkedik az Informatikai Osztály vezetője részéről ráosztott feladat ellátása érdekében az előírások betartása mellett.

21. Főigazgatóság vezetőinek informatikai biztonsággal összefüggő tevékenységét az informatikai referens támogatja, aki részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és hatáskörében intézkedik vagy javaslatot tesz a hibák kijavítására. Munkája során szorosan együttműködik az informatikai biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

22. Az informatikai referens feladatai és jogai:

a) a Főigazgatóság informatikai rendszerének olyan mértékű megismerése, hogy annak elemeit hatékonyan ellenőrizni tudja,
b) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
c) gondoskodik a jogszabályi előírásoknak megfelelő biztonsági osztályba sorolásról,
d) elvégzi vagy irányítja az *a)-c)* pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
e) előkészíti a szervezet elektronikus információs rendszereire vonatkozó szabályzatot,
f) összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében,
g) gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról, működtetéséről, jóváhagyásra előkészíti az éves informatikai biztonsági ellenőrzési tervet és jelen szabályzat javításait,
h) az Informatikai Osztály vezetőjével együttműködve felügyeli a biztonsággal kapcsolatban készítendő tervek és szabályzatok elkészítését,
i) informatikai biztonsági szempontból ellenőrzi az informatikai rendszer szereplőinek tevékenységét,
j) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
k) az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, és javaslatot tesz az Informatikai Osztály vezetőjének a további intézkedésekre,
l) új informatikai helyiség tervezése és kialakítása során ellenőrzi a jelen szabályzatban megfogalmazott, a helyiségek fizikai paramétereire vonatkozó követelmények kielégítését és a meglevő helyiségek paramétereinek értékét,
m) ellenőrzi az informatikai helyiségbe való beléptetési eljárást és a belépő személyek körének jogosultságát,
n) a Szervezeti és Működési Szabályzat (a továbbiakban: SZMSZ) rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét,
o) felügyeli az informatikai helyiségeket, eszközöket és infrastruktúrát érintő karbantartási terveket,
p) felügyeli a beruházásokat, a fejlesztéseket és az üzemvitelt informatikai biztonsági szempontból, és javaslatot tesz rájuk,
q) az új biztonságtechnikai eszközök és szoftverek tesztelésére ajánlást ad,
r) értékeli a rendszer eseménynaplóit,

s) ellenőrzi a víruskereső programok használatát,
t) ellenőrzi a dokumentációk meglétét és megfelelőségét (teljes körű, aktuális),
u) ellenőrzi, hogy a vonatkozó informatikai biztonsági követelményeket a rendszerek fejlesztési és az alkalmazási dokumentációiban is megjelenítik-e,
v) amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését,
w) az adott szakterületek vezetőivel egyeztetve meghatározza az egyes feladatkörökhöz tartozóan az informatikai biztonsággal kapcsolatosan elsajátítandó ismeretek körét, és ellenőrzi az elsajátítás tényét,
x) javaslatot tesz informatikai biztonságot erősítő továbbképzésre,
y) jelen szabályzatot évente felülvizsgálja, és javaslatot tesz a gyakorlati tapasztalatok, előfordult informatikai rendkívüli események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, valamint a fejlesztési és védelmi eljárások miatt szükségessé váló módosításokra,
z) javaslattételi joga van a fokozott és kiemelt védelmi osztályba sorolt informatikai rendszerek hozzáférési jogosultságainak kiadásában.

23. Jelen szabályzat vonatkozásában a felhasználó:
a) a munkavégzés során a rábízott eszközöket, szoftvereket felelősséggel, és az előírások, leírások, valamint az utasítások szerint használja és megőrzi,
b) az informatikai biztonsági szabályzatot megismeri és betartja,
c) részt vesz az informatikai oktatásokon,
d) a számítógépes munkavégzése során tiszteletben tartja a felhasználói csoportjára vonatkozó szabályokat és korlátozásokat, valamint a számítógépére megállapított házirendet,
e) a számítógépes rendszerekhez használt hozzáféréseit biztonságos módon megőrzi, a hozzáférésével elkövetett visszaélésekből és károkból származó következményekért a jogszabályokban rögzített mértékű felelősséggel tartozik,
f) jelzi az informatikai biztonsággal kapcsolatos észrevételeit,
g) informatikai segítséget kérhet, amennyiben olyan jellegű feladatot kell ellátnia, amelyhez nincs meg a megfelelő informatikai tapasztalata, és
h) a munkájához szükséges eszközöket, alkalmazásokat és szolgáltatásokat a szervezeti egysége vezetőjének engedélyével igényelheti.

24. Jelen szabályzat vonatkozásában a szervezeti egység vezetője:
a) a szervezeti egység dolgozóinak felvétele, távozása vagy munkakörváltozása esetén a szabályzatban meghatározott módon értesíti a változásról az Informatikai Osztályt vagy igazgatóságok esetén az igazgató által erre megbízott személyt,
b) gondoskodik arról, hogy a szervezeti egységének dolgozói megismerjék, és munkavégzésük során alkalmazzák a szabályzatot,
c) ellenőrzi, hogy a szervezeti egységének dolgozói betartják-e a szabályzatot,
d) informatikai kérdésekben dönt a szabályzatban részére delegált területeken (igénylések, engedélyek).

25. Jelen szabályzat tekintetében külső személynek (külső félnek) minősül azon természetes vagy jogi személy, aki a Főigazgatósággal kötött szerződéses kapcsolat keretében, a Főigazgatóság által kezelt vagy felügyelt területen, a Főigazgatóság megrendelésére informatikával kapcsolatos munkát vagy tevékenységet végez. Ilyen külső fél a Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ).

26. A külső személy munkája során az Informatikai Osztály, igazgatóság esetén – amennyiben az igazgatóság rendelkezik ilyen szakmai kompetenciával - az igazgató által erre megbízott személy gondoskodik a támogatásáról és felügyeletéről.

27. A külső személy (fél) munkavégzése során az Informatikai Osztály, igazgatóságok esetén az igazgató által erre megbízott személy a külső személy szerződéses kötelezettsége körében és személyes ellenőrzésen keresztül (kapcsolattartó) gondoskodik az alábbi követelmények teljesüléséről:

a) az informatikai rendszer integritása és az adatvédelem elvei nem sérülhetnek,
b) a hozzáférési jogot kapott partnerek (szervezetek, személyek) ezt a jogot tovább nem adhatják,
c) a hozzáférési azonosítókat (login név, jelszó stb.) a külső személynek (félnek) titkosan kell kezelnie, biztosítania kell, hogy azokhoz illetéktelenek ne férhessenek hozzá,
d) rögzíteni kell, hogy a hozzáférés bármely, a rendszer integritását sértő célból történő felhasználási kísérlete a hatályos jogszabályok szerint bűncselekménynek minősül,
e) amennyiben külső személy (fél) távolról éri el a Főigazgatóság hálózatát, vagy valamely informatikai rendszerét, akkor a biztonságos elektronikus adatcsere kapcsolat érdekében a külső fél köteles a Főigazgatóság által előírt biztonsági megoldásokat (pl. VPN kapcsolatot) megvalósítani mindazon saját eszközein, amelyekről a távoli elérés lehetséges.

28. Amennyiben a külső személy (fél) a szabályzat hatálya alá tartozó rendszerek vagy rendszerelemek vonatkozásában szolgáltatást nyújt, akkor

a) első lépésben részletesen meg kell határozni az érintett rendszerelemeket és az érintett folyamatokat,
b) ezt követően meg kell határozni azokat a paramétereket [pl. a normál üzemmódban minimálisan rendelkezésre álló eszközök számát, egyidejűleg működőképes eszközöket és operációs rendszer szoftvereket (típusonként), alkalmazások használóinak (típusonként) minimális számát, a maximális egyedi és átlagos kiesési időket, az üzemszerű módosítások átvezetésének maximális idejét, upgrade-ek követési idejét stb.], amelyeket a külső személyeknek el kell érnie ahhoz, hogy igazolható legyen a teljesítés.

29. Az Informatikai Osztály vezetőjének mérlegelnie kell a külső személlyel (féllel) kapcsolatos rendelkezésre állási kockázatokat is. Amennyiben ez a Főigazgatóság által nyújtott szolgáltatások folyamatosságához szükséges, a külső személlyel (féllel) olyan szerződést kell kötni, ami a megfelelő rendelkezésre állási kötelezettségeket tartalmazza.
30. A külső személyek (felek) által nyújtott szolgáltatások ellenőrzését rendszeresen kell végezni, és bármely felmerülő együttműködési probléma esetén ki kell deríteni annak okát. A hiba okának gyors és hatékony kiküszöbölése érdekében meg kell tenni a szükséges lépéseket.
31. A külső személlyel (féllel) kötött szerződésben meg kell határozni, hogy a szolgáltatást nyújtó külső személy nem-teljesítése, hibája, vétkessége esetén a Főigazgatóság milyen kompenzációra (pl. kötbér), vagy kártérítésre tarthat igényt, és azt milyen módon érvényesítheti.
32. A 31. pontban meghatározott rendelkezéseknek ki kell terjedniük a szerződés megszüntetésének, felmondásának eseteire is, és külön meg kell határozni a biztonsági előírások megsértése esetére vonatkozó szabályokat.

4. Az információ vagyon védelmének szabályai

33. A Főigazgatóság informatikai rendszeréről és eszközeiről csak az Informatikai Osztály szolgáltathat adatokat.
34. A Főigazgatóság döntése alapján bevezetett alkalmazói rendszerek bevezetésében és felhasználásában közreműködő külső személy (fél) titoktartási nyilatkozat tételére köteles. A titoktartási kötelezettség kiterjed az alkalmazói rendszerekkel kapcsolatos, és ezek bevezetése során tudomásra jutó információkra.

35. Az alkalmazói rendszerek bevezetése és működtetése kapcsán a rendszerekkel kapcsolatba kerülő külső személyeknek (feleknek) felelősséget kell vállalniuk azért, hogy
   a) a tudomásukra jutott információkat kizárólag a Főigazgatóság által meghatározott célokra használják fel,
   b) azokat harmadik személy részére a Főigazgatóság képviselőjének előzetes, írásos engedélye nélkül nem adják át, és
   c) a Főigazgatóság tevékenységére vonatkozó információk rögzítésére semmiféle technikai eszközt vagy más eszközt nem alkalmazhatnak.

36. Minden felhasználó az általa végzett elektronikus adatfeldolgozás során személyesen felelős az adatvédelmi szabályok és az információbiztonsági előírások betartásáért.

37. Külső személy (fél) munkavégzése során törekedni kell arra, hogy:
   a) a feladatához szükségtelen hivatali adat, információ ne kerüljön tudomására, valamint
   b) a feltétlenül szükséges adat birtoklásáról és az információ megismeréséről nyilatkozzon, és amennyiben szükséges, titoktartási nyilatkozatot tegyen.

38. Jelen szabályzat keretében alapvető munkakörnyezetnek a következőket tekintjük:
   a) a felhasználó részére biztosított munkaeszköz (számítógép, laptop) operációs rendszere,
   b) az irodaépületben (vidéki telephelyek esetén) kialakított informatikai hálózatban dedikáltan adatállományok tárolását végző rendszer (fájlszerver),
   c) opcionális rendszer (tartományvezérlés), amely elvégzi
      ca) a felhasználók azonosítását (címtár szolgáltatás),
      cb) a felhasználókra és a munkaeszközökre érvényes, kötelezően alkalmazandó szabályrendszer kikényszerítését (csoportházirendek alkalmazása),
      cc) a hálózati erőforrásokhoz való hozzáférésének szabályozását előre meghatározott jogosultsági rendszer alapján.

39. Az alapvető munkakörnyezetnek biztosítania kell a következőket:
   a) minden felhasználó részére elérhetőek legyenek a szervezeti egységének adatállományai olyan jogosultsági szinttel, ahogy azt az adott szervezeti egység vezetője írásban igényelte az Informatikai Osztálytól,
   b) minden felhasználó részére elérhető legyen az irodaépületben működő szervezeti egységek azon nyilvános adatállományai, amelyeket az adott szervezeti egységek közzétételi szándékkal az adott tárhelyen megosztanak, ezen tárhelyet a helyi informatikai rendszer mentésében, legalább naponta egyszer menteni kell,
   c) biztosítson egy elkülönített tárhelyet a felhasználónak a saját munkaeszközén, hogy a napi munkaanyagait igény szerint tárolhassa.

40. A Főigazgatóság számítógépeiről, szervereiről – a munkahelyi célú felhasználás kivételével – nem engedélyezett a programok, a minősített adatot tartalmazó adatállományok, illetve a munkavégzés során szerzett egyéb adatok, információk másolása, azok más, illetéktelen személyekkel történő megismertetése.

41. Nyomatképző berendezések (fénymásoló, nyomtató stb.) használata során törekedni kell a felesleges vagy rontott iratpéldányok megsemmisítésére.
Az előbbiekhez szükséges iratmegsemmisítő berendezések biztosítása és üzemeltetése, valamint a központi zúzásra szánt iratpéldányok gyűjtőedényeinek rendszeres ürítése a Vagyongazdálkodási és Üzemeltetési Főosztály, az igazgatóságokon az igazgató megbízottjának feladata.

42. Az információvédelem keretében törekedni kell a nyomatképző berendezések, biztonsági (szenzitív) nyomtatások, továbbá a fénymásoló berendezések, szkennelések lehetőség szerint biztonsági elemekkel történő kiegészítésére. A nyomtatás, másolás, szkennelés befejeztével kinyomtatott anyagot a nyomtatóból azonnal el kell vinni.

43. A műszaki eszközök (monitorok, nyomtatók, fénymásolók) elhelyezése során biztosítani kell, hogy bizalmas információ illetéktelen személy tudomására ne juthasson, és törekedni kell a

monitorok esetében az épület ellenőrizetlen közlekedő folyosóiról való teljes rálátás megakadályozására, hatékony megnehezítésére.
44. A 42. pontban előírt biztonsági nyomatképző funkciók használatával a felhasználó kizárólagos felelőssége az iratpéldányok biztonságos kezelése, elhelyezése.
45. Amennyiben a felhasználó gondatlanságból vagy szándékosan a 41. pontban leírtaknak megfelelően nem gondoskodik a felesleges vagy rontott iratpéldányok megsemmisítéséről és így az iratpéldány illetéktelen kezekbe kerül, vagy az iratokban lévő információkat illetéktelen célra felhasználták, a felhasználó ezért teljes felelősséggel tartozik.
46. Az adathordozók és nyomtatványok tárolása során gondoskodni kell az illetéktelen személyek hozzáférésének megakadályozásáról.
47. A 46. pontban meghatározott elvnek megfelelően a felhasználónak kötelessége az irodájában található zárható tároló eszközöket igénybe venni, s azoknak a kulcsát biztonságosan tárolni, amikor a felhasználó munkakörnyezete (irodája, íróasztala, irodában található tárolók) felügyelet nélkül marad.
48. Az IT biztonsággal szemben támasztott követelmények:
a) Rendelkezésre állás: a szolgáltatások és adatok elérhetősége biztosított legyen az arra jogosult felhasználók számára. Biztosított a védelem a jogosulatlan hozzáféréstől és adatmódosítástól, törléstől, és a szolgáltatás elérhetőségének megakadályozásától.
b) Sértetlenség: adat- és rendszerintegritás. Adatintegritással került biztosításra, hogy adat nem módosulhat nem engedélyezett (nem tervezett) módon a tárolás, feldolgozás, adatátvitel során. Rendszerintegritás alapján a rendszer a megvalósított funkciót nem engedélyezett manipulációtól mentesen hajtja végre.
c) Bizalmasság: az a követelmény, hogy a bizalmas, vagy magántermészetű információ nem jut jogosulatlan személy kezébe. Ez vonatkozik az adat tárolására, feldolgozására, átvitelére egyaránt.
d) Felelősség: bármely entitás cselekvései követhetőek legyenek, és egyértelműen visszavezethetőek legyenek rá.
e) Megbízhatóság: a különböző biztonsági intézkedések az irányítási, technológiai, működési vezérlés területén megfelelően működnek, és védik a rendszert és az általa feldolgozott adatot. Előbbi célok megvalósítottnak tekinthetők, amennyiben:
ea) a kívánt funkció jelen van és pontosan megvalósított,
eb) megfelelő védelem van a nem szándékos hibák ellen, és
ec) megfelelő védelem van a szándékos hibák (behatolás, stb.) ellen.
49. A Főigazgatóság területén végzett minden tevékenység (pl. építési és karbantartási munka, ügyfélforgalom bonyolítása, üzemeltetési feladatok ellátása, postaszolgálat, futárszolgálat stb.) során figyelemmel kell lenni jelen szabályzat betartására és betartatására, az IT biztonság követelményeinek maximális fenntartására.
50. A Főigazgatóság központi szervezeti egységében és igazgatóságain végzett minden tevékenység során szem előtt kell tartani
a) a képzések hallgatói és a projektek által támogatott egyének adatainak és információinak, valamint
b) az ügyük elemeinek bizalmas jellegét, és ezért az informatikai struktúrát és környezetet ennek megfelelően kell kialakítani.
51. Számítógép- vagy programhibából eredő adatvesztés gyanúja esetén – az adatfeldolgozás szüneteltetése mellett – a kijelölt informatikust haladéktalanul értesíteni kell. Az értesítés módja személyes, telefonos értesítés vagy elektronikus úton tett bejelentés. A probléma tisztázása után az informatikus útmutatása szerint kell lefolytatni az adatrögzítést és adatfeldolgozást.
52. Az alkalmazásokhoz és a hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése útján gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, és ne törölhesse.

53. A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sértetlenségét, valamint a véletlen vagy szándékos törlések elleni védelmét.
54. Az Informatikai Osztály feladata biztosítani az informatikai rendszerek folyamatos rendelkezésre állását az alábbi eszközök felhasználásával:
a) rendszeres adatmentésekkel és szoftvertelepítő készletek megfelelő biztosításával és megfelelő tárolásával,
b) szünetmentes tápellátást biztosító berendezések üzemeltetésével és karbantartásával,
c) tartalék eszközök és alkatrészek biztosításával, valamint
d) helyreállítási módszerleírások, vészforgatókönyvek naprakész biztosításával.
55. A rendszerek információvagyonának biztonsági szempontú osztályozása az adatok bizalmassága, megőrzési követelményei és hitelessége szempontjából történik.
56. Az adatokat az alábbi szempontok szerint kell osztályozni:
a) a közérdekű, illetve a közérdekből nyilvános adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.), majd a GDPR, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) határozza meg.
b) a közérdekű adat nyilvánosságához fűződő jogok minősítéssel történő korlátozását a minősített adat védelméről szóló 2009. évi CLV. törvény szabályozza,
c) az üzleti titok körébe tartozó adatokat a Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:47. §-a határozza meg,
d) az adatok osztályozója, amennyiben azt jogszabály nem szabályozza, annak a szervezeti egységnek a vezetője, amelynek érdekkörébe az adat tartozik,
e) a d) pont alapján rögzíteni kell, hogy a szervezeti egység vezető nem csak osztályozója, hanem gazdája is az adatnak,
f) a rendszerekben nyilvánosnak csak a Főigazgatóság vezetése által egyértelműen annak minősített információ tekinthető, és
g) a nyilvános adatok kivételével valamennyi adatot bizalmasként (védendő nem titkos adat) kell kezelni.
57. Az adatkezelésre vonatkozó szabályokat az Info tv. tartalmazza.
58. Az informatikai adatkezelés és adatfeldolgozási munka során az adatvédelemre vonatkozó szabályok szerint kell eljárni.
59. Az egyes közérdekű adatok közzétételének feladatai a Főigazgatóság internetes honlapjának (www.tef.gov.hu) vonatkozásában azt a hivatali szervezeti egységet terhelik, amely azokat előállította, illetve amelynek működése során, vagy ahhoz kapcsolódóan keletkeztek, illetőleg amely összefügg a feladat- és hatáskörébe tartozó feladataival.
60. A Főigazgatóság internetes honlapjának kezelését az Informatikai Osztály vagy egy megbízott külsős cég kezeli.
61. A honlapot kezelő feladata a közzétételi felelőstől kapott adatokat a honlapon megjeleníteni oly módon, hogy adatok védelme biztosított legyen a jogosulatlan megváltoztatás, törlés, megsemmisülés és sérülés ellen.
62. A Főigazgatóság honlapja az adat közzétételével, helyesbítésével, frissítésével vagy eltávolításával kapcsolatban az esemény bekövetkeztének dátumát és időpontját, valamint az esemény kiváltásában közreműködő felhasználó nevét naplózza. A naplóról rendszeresen biztonsági másolat készítése a honlapkezelő feladata.
63. A Főigazgatóság informatikai hálózatára kizárólag a NISZ által biztosított eszközöket (számítógépeket, laptopokat, mobil eszközöket) lehet rácsatlakoztatni.

64. A 63. pont alapján a Főigazgatóság informatikai hálózatára csatlakoztatott eszközökön helyi vagy központi megoldással (központi címtárral) biztosítani kell, hogy az eszközöket kizárólag felhasználónév és jelszó (mobil eszköz esetén PIN kód) megadása után (felhasználói azonosítás és hitelesítés) lehessen használni.
65. A helyi és a központi felhasználói adatokat úgy kell megalkotni, hogy a felhasználóhoz tartozó objektum tartalmazzon egy rövid felhasználónevet (javasolt névkonvenció: vezetéknév és a keresztnév kezdőbetűi), valamint a felhasználó teljes nevét (mint megjelenítendő nevet).
66. Rendszergazdai feladatokat kizárólag a NISZ jogosult elvégezni. Ebbe beletartozik a felhasználói számítógépek biztosítása, azokra szoftverek telepítése, vállalati levelezőrendszer futtatása.
67. A 63. pontban foglaltak mellett külön engedéllyel, szakmailag indokolt esetben csatlakoztatható a felhasználó saját tulajdonában lévő eszköz a Főigazgatóság informatikai hálózatára. A szakmai indok ellenőrzése az Informatikai Osztály vezetőjének a hatásköre.
68. A Főigazgatóság informatikai hálózatában az internet kijárat védelme érdekében biztonsági és védelmi megoldásokat kell alkalmazni.
69. A biztonsági megoldások során gondoskodni kell a hálózat fizikai elemeinek védelméről:
a) a vezetékek és végpontok illetéktelenek általi hozzáférésének megakadályozásáról,
b) vezeték nélküli kapcsolatok megfelelő titkosításáról,
c) vezeték nélküli kapcsolódások megfelelő felügyeletéről és kezeléséről (pl. a kapcsolódó eszközök fizikai címének ellenőrzéséről és azok engedélyezéséről vagy tiltásáról), valamint
d) az eszközhöz való illetéktelen hozzáférés megakadályozásáról.
70. A 69. a)-d) pontjában leírt védelem megvalósíttatása az Informatikai Osztály feladata.
71. A központi szervezeti egységnél (budapesti telephelyek) a NISZ, az igazgatóságokon az Informatikai Osztály gondoskodik az elektronikus informatikai rendszerek behatolás elleni védeleméről (tűzfal), az erre vonatkozó szakmai előírások és a biztonsági szabályok betartása mellett.
72. A 71. pontban előírt védelmi eszköz (tűzfal) üzemeltetése, amennyiben üzemeltetési-szakmai szempontból indokolható, külső partnernek megfelelő dokumentáltság és felügyelet mellett írásos megegyezéssel átadható. Alapértelmezetten a központi szervnél és az igazgatóságokon üzemeltetendő védelmi eszköznek a központi szervezeti egységnél a NISZ, az igazgatóságokon az Informatikai Osztály üzemeltetésében kell lennie.
73. Alapszabályként a védelmi berendezésnek (tűzfalnak) a beérkező hálózati kapcsolatokat blokkolnia kell.
74. Azon hálózati kapcsolatokat, amelyek a Főigazgatóság működése szempontjából indokoltak, átjutásukat a tűzfalon engedélyezni és naplózni kell. A naplónak a hálózati tárkapacitástól függően, lehetőség szerint 30 napig visszamenőleg tárolni kell.
75. Minden engedélyezett kapcsolatot szakmai indoklással együtt a hálózati dokumentáció mellékleteként rögzíteni kell. A dokumentációt az informatikai biztonsági referens részére elérhetővé kell tenni.
76. Amennyiben az elektronikus információs rendszerben biztonsági incidens történik, úgy a védelmi berendezések napló állományait az Informatikai Osztály, valamint az informatikai biztonsági referens részére be kell küldeni.
77. A központi informatikai rendszereket automatikus vírusvédelmi rendszerrel kell ellátni, amelyek üzemeltetését és felügyeletét a budapesti telephelyeken a NISZ, az igazgatóságokon az Informatikai Osztály látja el.
78. Szerverek esetén alkalmazandó vírusvédelmi eljárások:
a) Minden szerverhez, amelyhez kereskedelmi forgalomban beszerezhető vírusvédelmi szoftvert lehet beszerezni, azt telepíteni kell. Továbbá biztosítani kell, hogy a

szerveroldali vírusvédelmi szoftver, víruskereső motor és vírusminta adatbázisa automatikusan frissüljön.

b) A levelező szerver esetében a levelezésért felelős alkalmazásba beépülő, a levélforgalom vizsgálatát végző vírusvédelmi szoftvert kell alkalmazni.

79. Az elektronikus levelezés biztonsági irányelveinek érvényesítéséről a levelező rendszer üzemeltetője felelős. Az irányelvek a következők:

a) a folyamatos üzembiztonság megvalósítása,

b) az elektronikus küldemények adatintegritásának megtartása,

c) a levelezőrendszer vírusvédelmének biztosítása és folyamatos frissítése, és

d) az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelme [szoftverfrissítések, service pack-ok (javító csomagok) és Security-patch (biztonsági javítás) fájlok telepítése].

80. Az Informatikai Osztály által felügyelt területen és szervezeti egységeknél informatikai hálózatot, vezetékes vagy mobil internet kapcsolatot csak az Informatikai Osztály engedélyezhet, hagyhat jóvá és hozhat létre. A Főigazgatóság által biztosított mobil előfizetésekhez tartozó adathozzáférés az Informatikai Osztály által jóváhagyott mobil internet kapcsolatként értelmezendő.

81. A használatra kapott számítógép rendszerszintű beállításainak – ideértve az irodai programok felhasználói beállításait is – módosítása nem engedélyezett.

82. A felhasználónak tilos a vírusvédelmi programot inaktívvá tenni, a beállításokat megváltoztatni, a vírusvédelmet eltávolítani.

83. A vírussal fertőzött fájlt vagy elektronikus adathordozót bármilyen formában továbbítani, továbbadni, vagy fertőzött állománnyal munkát végezni szigorúan tilos.

84. A Főigazgatóság informatikai rendszerébe és informatikai eszközére csak azt a szoftvert szabad telepíteni és használni, amelyik:

a) a Főigazgatóság által jóváhagyott, telepítésre kiadott és engedélyezett nyílt forráskódú szoftver, vagy

b) szerzői jog szerint biztosított licencigazolással, vagy más jogi igazolással rendelkező, és tulajdonosi vagy felhasználási szerződéssel biztosított hivatalos forrásból származó jogtiszta szoftver.

5. A humánerőforrásokra vonatkozó biztonsági szabályok

85. Jelen szabályzat hatálya alá eső személyekre a következő, általános kötelezettségek érvényesek:

a) az informatikai rendszerek használata alapértelmezetten a hivatalos célokra engedélyezett,

b) a munkáltató jogosult a hivatali munkavégzéshez biztosított munkaeszközön (számítógép, laptop, táblagép, mobiltelefon), illetve a hivatali elektronikus postafiók adatainak ellenőrzésére, amennyiben az ellenőrzést a munkáltató jogos érdeke a hivatali ügymenet folyamatosságának biztosításához, valamint információbiztonsági, illetve adatvédelmi biztonsági incidens kivizsgáláshoz megkívánja,

c) a munkáltatói jogkör gyakorlója a b) pontban megfogalmazottak alapján, kötelezően jegyzőkönyv készítése mellett ismerheti meg a felhasználó azon magánadatait, amelyet a jelen szabályzatban meghatározott módon, külön mappában kerültek eltárolásra. Magánlevél, illetve magán dokumentum tartalma abban az esetben ismerhető meg, ha a levél vagy a dokumentum meghatározó/leíró adatai (levél esetében a küldője/címzettje, tárgya, illetve a mellékletek elnevezése; dokumentum esetén az állomány neve, mérete, állomány típusa stb.), illetve ezek keletkezésének/létrehozásának körülményei

biztonsági incidens gyanújára adnak okot. A jegyzőkönyvnek tartalmaznia kell a magánadatok ellenőrzésének indoklását (célját) is.

d) a b) és a c) pontban leírtaknak megfelelő módon bármely felhasználó munkaeszközén és elektronikus postafiókjában tárolt adatok magánjellegű adatok és dokumentumok megismerésének joga az informatikai biztonsági referenst is megilleti,
e) a használt informatikai eszközpark kezelésével kapcsolatos kezelési és biztonsági ismereteket el kell sajátítani, és készség szintjére kell fejleszteni,
f) a rendszerekbe csak szabályszerűen, a személyes felhasználó-azonosító kóddal szabad bejelentkezni,
g) az informatikai rendszerekben csak azokat a feladatokat szabad elvégezni, amelyek a felhasználó vagy üzemeltető munkájának ellátásához szükségesek, függetlenül attól, hogy a rendszer esetleg ennél szélesebb körű tevékenységet enged meg,
h) minden személynek biztosítania kell, hogy felhasználó-azonosítóját és jelszavát más felhasználók ne tudják használni,
i) a képernyőket, nyomtatókat úgy kell elhelyezni, hogy azok minél kevesebb lehetőséget biztosítsanak illetéktelen betekintésre,
j) a Főigazgatóság által rendszeresített biztonsági funkciókat (pl. az automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos,
k) a Főigazgatóság eszközein csak a Főigazgatóság által engedélyezett eszközöket és programokat szabad használni,
l) tartózkodni kell minden olyan tevékenységtől, amely az informatikai rendszerben kárt okoz a biztonság, a sértetlenség és teljesítmény terén,
m) az információtechnológiai biztonságra és az adatvédelemre vonatkozó minden egyéb utasítást és jogszabályt maradéktalanul be kell tartani,
n) esetleges meghibásodás esetén törekedni kell a további károsodás megelőzésére (a hiba jelentésével, a további használat mellőzésével stb.),
o) a felhasználónak vagy üzemeltetőnek ismernie kell a segítségkérés és hibajelentés módját, amennyiben ez az ismeret nem áll rendelkezésére, hiba esetén értesítenie kell a munkahelyi vezetőjét, külső személyek esetén a Főigazgatóság kijelölt kapcsolattartóját,
p) az informatikai biztonságot veszélyeztető eseményről vagy ennek gyanújáról értesíteni kell az informatikai biztonsági referenst, informatikust és a munkahelyi vezetőt, külső személyek esetén a Főigazgatóság kijelölt kapcsolattartóját,
q) a közvetlen munkahelyi vezető (külső személyek esetén a Főigazgatóság kijelölt kapcsolattartója) a felelős azért, hogy a fenti szabályokat az érintettekkel ismertesse.

86. Az adatvédelem és az adatbiztonság szabályairól szóló szabályzat alapján az adatok megismerését – az adat megismeréséhez és a megismerhetőség kizárásához fűződő közérdek súlyának mérlegelésével – az azt kezelő szerv vezetője engedélyezheti. A döntés meghozatala előtt el kell végezni az érdekmérlegelési eljárást, az alábbi szempontrendszer alapján:

a) a tervezett adatkezelés megkezdése előtt át kell tekinteni, hogy a célja elérése érdekében feltétlenül szükséges-e az adat kezelése,
b) rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél,
c) meg kell határozni a kiemelt ügy zártan kezeléséhez fűződő jogos érdeket,
d) meg kell határozni, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek,
e) meg kell határozni, hogy mik lehetnek azok nyilvánossághoz fűződő érdekek az adott adatkezelés vonatkozásában, melyek azok a szempontok, amelyeket a nyilvánosságára való hozatalt kérők felhozhatnának a zárt adatkezeléssel szemben,

f) meg kell határozni, hogy miért korlátozza arányosan a Főigazgatóság jogos érdeke – és az ennek alapján végzett adatkezelés – a nyilvánosság biztosításhoz fűződő jogokat.

87. A felhasználó vagy az informatikus a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja.

88. A felhasználó jelszókezelési szabályai:

a) a felhasználói jelszavaknak minimum hossza 8 karakter összetétele kötelezően: kisbetű, nagybetű, szám kombinációja.
b) jelszavak nem hozhatók nyilvánosságra,
c) a jelszavak biztonságának megőrzéséért a felhasználó személyesen felel,
d) a felhasználó a jelszavát nem oszthatja meg senkivel,
e) amennyiben a felhasználónak a legkisebb gyanúja is felmerül, a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az informatikai biztonsági referenst, valamint az Informatikai Osztályt értesíteni.
f) más felhasználó azonosítóját átmeneti jelleggel sem szabad használni, valamint
g) a felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.
h) a felhasználói jelszavaknak minimum 8 karakterből kell állnia, kisbetű, nagybetű, szám kombinációjából kell állnia

89. A szakmai feladatok hatékony ellátásához szükséges információkhoz, szolgáltatásokhoz való hozzáférés érdekében a Főigazgatóság valamennyi felhasználója jogosult a munkahelyi internet, és elektronikus levelezés használatára.

90. Az internet szolgáltatásait a munkahelyi eszközökön (azaz a Főigazgatóság által biztosított eszközökön) alapvetően a munkaköri feladatok ellátására lehet igénybe venni, a személyes célú használat megengedett munkaközi szünetben.

91. Alapelv, hogy minden weblap és internetes szolgáltatás elérése engedélyezett, amíg annak tartalma nem ütközik semmilyen jogszabályi előírásba.

92. Tekintettel arra, hogy az internethasználat a Főigazgatóság által biztosított infrastruktúrán, és szolgáltatási költségen valósul meg, a Főigazgatóság jogosult bármikor, bármilyen weblap, internetes szolgáltatás elérésének ideiglenes vagy teljes korlátozására. Ezen weboldalak nem ütköznek semmilyen jogszabályi előírásba, letiltásuk a hálózat leterheltségének kezelhetőségére, a munkaidő hatékony kihasználására irányul.

93. A hálózat számára nagy terhelést jelentő képi- (pl. grafikus fájl, video) és hangi- (pl. *.mov, *.mp3, *.avi, *.wav. stb.) információkat tartalmazó anyagok letöltése, továbbítása csak az Informatikai Osztállyal, igazgatóság esetén az igazgatóság igazgatójával előzetesen egyeztetve engedélyezett.

94. A felhasználók a Főigazgatóság nevében nem tölthetnek fel engedély nélkül az internetre adatot és anyagot (pl. honlap, hirdetmények).

95. A Főigazgatóság tulajdonát képező szoftverek interneten vagy e-mailen keresztül történő továbbítása, mások részére való hozzáférhetővé tétele – előzetes külön engedély hiányában – nem engedélyezett.

96. A Főigazgatóság felhasználóira az interneten történő viselkedésre, megnyilvánulásokra a Magyar Kormánytisztviselői Kar Hivatásetikai Kódexében megfogalmazott alapelvek érvényesek.

97. Tiltott tartalmú oldalak:

a) szexuális tartalmú oldalak, különösen az alábbi tartalmakkal:
   aa) kiskorúak veszélyeztetése,
   ab) erőszak,
   ac) pornográfia,
   ad) marketing molesztáló jellegű formái (felhívás ilyen jellegű oldalak látogatására),
b) az emberi méltóság megsértése,
c) rasszizmus,

d) szexuális beállítódás, vallás, nemzetiség vagy etnikai származás miatti megkülönböztetés,
e) gazdasági bűnözés fogalma alá eső cselekmények,
f) csalás,
g) tiltott kereskedelmi tevékenység,
h) hitelkártyával való visszaélésben való közreműködés,
i) rémhírterjesztés,
j) információbiztonság veszélyeztetése,
k) rossz szándékú hackertámadás,
l) hacker, cracker technológiák és leírásuk, eszközök terjesztése, használata,
m) vírusprogramok terjesztése, írása,
n) a magánszféra megsértése,
o) személyes adatokkal való visszaélés,
p) elektronikus zaklatás,
q) a személyiségi jogok megsértése,
r) rágalmazás,
s) meg nem engedett összehasonlító reklám,
t) a szellemi tulajdon megsértése,
u) tiltott szerencsejáték,
v) a szerzői jog által védett digitális anyagok (művek, szoftverek, zenék stb.) jogosulatlan terjesztése,
w) bombák készítéséhez adott segítségnyújtás,
x) illegális kábítószer használat, előállítás és terjesztés,
y) nemzetbiztonsági szempontból tiltott tartalmú oldalak,
z) terrorista tevékenység.

98. A tiltott tartalmú oldalak tiltása tartalomszűrő megoldással történik. A tartalomszűrő működésének biztosítása és a szűrő szükség szerinti bővítése NISZ feladata.
99. Amennyiben a felhasználó az internetes portálok használata közben véleménye szerint olyan oldalt ér el, amely a 97. pontban felsorolt tartalmak valamely kritériumának megfelel, a szervezeti egység vezetőjének javasolhatja, hogy a NISZ módosítsa a tiltott tartalmú weboldalak listáját, így biztosítva a sértő tartalom elérhetetlenségét.
100. A tiltott weboldalak listáján szereplő internetes oldal megnyitásának kísérlete nem minősül szabálysértésnek, mivel az nem ütközik semmilyen morális, erkölcsi vagy törvényi szabályba.
101. A Főigazgatóság elektronikus levelezőrendszert biztosít a szervezete, valamint a Főigazgatósággal munkavégzésre irányuló jogviszonyban álló felhasználók részére, amelyet alapvetően a hivatalos munkavégzéshez biztosít. Az elektronikus levelezőrendszer külső szolgáltató általi szolgáltatásként biztosított.
102. Az elektronikus levelező rendszerben megjelenő információk, dokumentumok, elektronikus levelek a Főigazgatóság tulajdonát képezik, figyelembe véve a személyes adatok kezelésére vonatkozó hatályos adatvédelmi szabályokat, eljárásokat.
103. A Főigazgatóság által a felhasználó részére biztosított, a munkavégzését segítő elektronikus levelező postafiókot magáncélra használni bizonyos feltételekkel, formai követelményekkel engedélyezett.
104. A magáncélú leveleket a postafiók könyvtárstruktúrájában láthatóan el kell különíteni a felhasználó által folytatott hivatalos levelezéstől (magánlevelezés nevű könyvtárba a beérkezett üzenetek, és az elküldött üzenetek könyvtáraktól elkülönítve), a küldött és fogadott levelek fejlécét el kell látni a „[PRIVATE]" (azaz magáncélú) megjelöléssel. A megjelölés alapján az elektronikus levelet megilleti a levéltitok védelme.
105. A magáncélú levél nem tartalmazhatja a Főigazgatóság hivatalos elektronikus levélhez kötött aláírását.

106. A 104. pontban megjelölt könyvtárban található elektronikus levelek fejlécét tartalmazó listát a Belső Ellenőrzési Osztály által indított vizsgálat keretében bármikor lekérhető, annak tartalmát a Főigazgatóság adatvédelmi és adatkezelési szabályai alapján kell tárolni.
107. A munkatársak kérhetik a Főigazgatóság által biztosított levelezésnek a tulajdonukban lévő, és a munkáltató által engedélyezett mobil eszközre való beállítását.
108. Amennyiben a vállalati levelezés saját tulajdonú mobil eszközre lett beállítva, úgy ezen az eszközön is alkalmazni kell a Főigazgatóság által előírt biztonsági intézkedéseket (PIN kód, jelszavas képernyőzár). Ezek hiányában az Informatikai Osztály munkatársa a vállalati levelezés beállítására irányuló kérést köteles megtagadni.
109. A Főigazgatóságról távozó felhasználó postafiókjának archiválásáról, megszüntetéséről, valamint a megszüntetéséig a betekintési jogosultak köréről a távozó felhasználó szervezeti egységének vezetője jogosult dönteni, ez alól kivétel a felhasználó által elkülönített, magáncélú levelezését tároló könyvtár.
110. A távozó felhasználó postafiókjáról a felhasználó szervezeti egységének vezetőjének döntése alapján archivált állomány készülhet. Az archív leveket tartalmazó állományt a kiléptetést végző NISZ a kért tárhelyre másolja. Ezen adatállományokat a tároló kapacitás függvényében, azonban lehetőség szerint legalább 2 évig a szerveren kell tárolni.
111. A felhasználó postafiókjának teljes vagy részleges tartalma a felhasználótól elkérhető, vagy szükség esetén az Informatikai Osztály bevonásával lekérhető az alábbi körülmények fennállásakor:

a) a Belső Ellenőrzési Osztály, által folytatott vizsgálatok esetén a vizsgálatok lebonyolításához szükséges információk megszerzésére vonatkozóan:
   aa) a vizsgálat célzott, így az adatok bekérése is (vizsgált időperiódus vagy egyéb konkrét feltétel),
   ab) első lépésben a postafiók leveleinek fejlécét, a fejléci információk alapján pedig a vizsgálatot végző szervezeti egység a vizsgálat céljának megfelelően kiválasztott levelek nyomtatott verzióját, beleértve a levél mellékleteit is,
   ac) a levelezésből kinyert információk kezelésére, tárolására és megsemmisítésére a szervezeti egységek belső szabályai, valamint a Főigazgatóság adatvédelmi és adatkezelési szabályai az irányadóak,
b) külső nyomozati szerv által történt nyomozati cselekményben való részvétel, hivatalos megkeresése esetén a nyomozati szerv által kért részletességgel [csak fejléc, nyomtatott forma (mellékletekkel), elektronikus másolat].

112. Az elektronikus levelezés során a postafiókokat vírusvédelmi rendszer védi. Az elektronikus postafiókba érkező, ismeretlen feladótól (gyanús, értelmezhetetlen vagy külföldi) származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, vagy idegen nyelvű küldeményekkel – a fennálló vírusveszély miatt – fokozott óvatossággal kell eljárni. A gyanús küldemény érkezésekor, valamint a vírusvédelmi rendszer riasztása esetén haladéktalanul értesíteni kell az Informatikai Osztály munkatársait ezzel egyidőben a NISZ ügyfélszolgálatán keresztül bejelentést kell tenni. A csatolmányt ilyen esetben tilos megnyitni.
113. A felhasználó elektronikus levelezési címével beregisztrálni bármely, az interneten lévő webes rendszerbe, vagy külső szervezet rendszerébe csak szakmailag indokolt esetben és a közvetlen vezetője hozzájárulásával engedélyezett.
114. Tilos lánclevelek indítása vagy továbbítása.
115. A Főigazgatóságnak a mobiltelefon használatának rendjéről szóló szabályzatában (a továbbiakban: mobiltelefon szabályzat) elfogadott elvek szerint a Főigazgatóság munkatársai számára mobiltelefon elérhetőséget biztosíthat.
116. A mobiltelefon szabályzatban előírt felhasználási keretösszeget a felhasználó hivatalos és személyes célra használhatja. A hívások listája nem kérhető le.

117. A munkatársak a számukra biztosított mobiltelefonnal munkaidőben jogosultak az Informatikai Osztály által biztosított vezeték-nélküli hálózat igénybevételére.
118. A munkatársak a saját tulajdonú mobiltelefonnal is jogosultak a 117. pontban biztosított vezeték nélküli hálózatra. Ezen jogot a főigazgató bármikor, indoklás nélkül visszavonhatja.
119. A mobiltelefonról indított internetezési szabályokat jelen szabályzat 39. §-a tartalmazza, azzal a kiegészítéssel, hogy a mobiltelefonon alapesetben nincsenek korlátozott weboldalak.
120. A mobiltelefonról indított internetes forgalom listája alapesetben nem kérhető le, kivétel, ha a munkáltató megfelelő dokumentáltsággal és céllal teszi.
121. A mobiltelefon tárolókapacitása mind hivatalos, mind személyes célra felhasználható.
122. Azok a mobiltelefonok, amelyek bármilyen, a Főigazgatósághoz köthető adatot, információt tartalmaznak (hivatali végleges, vagy munkadokumentum, fénykép, hivatali elektronikus levelezés), kizárólag jelszavas, és időzáras billentyű- vagy képernyőzárral használhatóak.
123. Az új belépő dolgozót az illetékes szervezeti egység vezetője utasítja a szükséges informatikai biztonsági szabályok megismerésére, és tájékoztatja az informatikai szabályzatok elérhetőségéről. Az informatikai szabályzatok megismerésének tényét a dolgozó aláírásával igazolja.
124. Minden felhasználó köteles a vonatkozó informatikai-szakmai szabályzatokat megismerni és betartani, és köteles ezek betartása során az informatikai rendszer használatát irányító személyekkel együttműködni.

6. Az informatikai biztonsági incidensek kezelése

125. Az informatikai rendszereket érintő (vagy vele összefüggésbe hozható), bármilyen bekövetkezett, vagy előre látható biztonsági eseményt (betörés, lopás, tűz, víz, villámcsapás, balesetveszélyes eszköz, eszköz elvesztése vagy eltűnése stb.) az Informatikai Osztály felé az eseményt észlelőnek azonnal jelezni kell
126. Betörés, lopás esetén kötelezően hatósági (rendőrségi) bejelentést kell tenni.
127. A felhasználó köteles jelezni az Informatikai Osztálynak, az igazgatóságoknál az igazgatónak (vagy az általa ezzel megbízott munkatársnak) bármely, az informatikai biztonságot érintő gyanús eseményt (pl. előző nap lekapcsolt, azonban reggel bekapcsolva talált gépet), vagy ezzel kapcsolatos gyanúját.
128. Az informatikai rendszereket érintő (vagy vele összefüggésbe hozható) biztonsági eseményeket az alábbi módon kell bejelenteni:

a) felhasználói hiba észlelése esetén haladéktalanul értesíteni kell telefonon vagy személyesen az Informatikai Osztály munkatársát, igazgatóságoknál az igazgatóját (vagy az általa ezzel megbízott munkatársat),
b) biztonsági esemény esetén haladéktalanul telefonon értesíteni kell Informatikai Osztály vezetőjét, igazgatóságoknál az igazgatót, aki az esemény jellegétől függően intézkedik, indokolt esetben tájékoztatja a főigazgatót.

129. Az eseményt követően az eseményről jegyzőkönyvet kell készíteni, és azt Informatikai Osztály részére írásban el kell küldeni (e-mail, levél). A jegyzőkönyvben rögzíteni kell az esemény részleteit, körülményeit.
130. Az informatikai rendszer bármely felhasználói pontján jelentkező, a hálózattal, eszközzel, vagy adott alkalmazással kapcsolatban felmerülő rendellenes működés, jelenség, vírusjelzés, futtatási hiba esetén a felhasználó köteles a tapasztalt jelenséget, és amennyiben van, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul bejelenteni az informatikai biztonsági referensnek.

131. Az informatikai biztonsági referens a biztonsági incidenst kivizsgálja és az Informatikai Osztály bevonásával intézkedést, vagy ezzel párhuzamosan szükség szerint változtatást javasol jelen szabályzat vonatkozásában. Az Informatikai Osztály vezetője, igazgatóság esetén az igazgató által kijelölt személy a hiba elhárítása érdekében intézkedik, és a probléma elhárítását elvégzi. A hiba megszüntetéséről és a további teendőkről a felhasználót folyamatosan tájékoztatja, valamint helyettesítő eszköz biztosításával gondoskodik a felhasználó munkavégzési lehetőségéről.

132. Az informatikai rendszer rendellenes működése vagy a biztonságot veszélyeztető esemény elhárítása érdekében az informatikai eszközök használatát, a hálózat működését, az internet és levelezés használatát az Informatikai Osztály, igazgatóságoknál az igazgató részben vagy egészében korlátozhatja vagy leállíthatja.
133. Jelen szabályzatban leírt internethasználat és elektronikus levelezés szabályainak a felhasználó általi megszegése esetén az érintett személy ellen, belső vizsgálat indul. Az Informatikai osztály, belső ellenőr és az informatikai szolgáltató bevonásával.

7. A fizikai és környezeti infrastruktúra biztonsága

134. Az informatikai infrastruktúra elemeinek és a helyiségeknek a kockázatokkal és a tágabb értelemben vett értékükkel arányos fizikai védelmet kell biztosítani.
135. Informatikai helyiségeknek minősülnek azon helyiségek, amelyek működő szerverek és hálózati elosztó elemek (router, switch) elhelyezésére és működtetésére szolgálnak. Kivételt képeznek azon egyéb helyiségek, amelyekben zárt, kulccsal biztosított rack szekrény található.
136. Az informatikai helyiségekbe való belépési jogosultságot személyre szólóan, az adott személy feladata alapján kell meghatározni. Állandó vagy egyedi belépési jogosultságot az informatikai helyiségbe az Informatikai Osztály vezetője, igazgatóságoknál az igazgató adhat.
137. Az IT eszközök szállítása esetén a megbízott személy vagy cég teljes mértékben felel az IT eszközért.
138. A belépési jogosultsággal nem rendelkezők az informatikai helyiségben csak az arra jogosultak felügyelete mellett tartózkodhatnak.
139. Abban az esetben, amennyiben az informatikai helyiségbe (pl. szerverszoba) valamilyen okból (szemle, ellenőrzés, szerelés stb.) belépési jogosultsággal nem rendelkező személynek be kell jutni, arról előzetes egyeztetés mellett a kijelölt informatikus gondoskodik.
140. Tilos az informatikai helyiségben a helyiség funkciójától eltérő anyag vagy eszköz tárolása.
141. Az informatikai helyiségek számítógépeire telepített szoftverek karbantartását a NISZ munkatársai, az igazgatóságokon az Informatikai Osztály kollégái végzik.
142. Az informatikai eszközök nyilvántartásáért az Informatikai Osztály tartozik felelősséggel. A kijelölt informatikus az eszközöket az informatikai eszköznyilvántartásban tartja nyilván és a változásokat lehetőség szerint azonnal, de legkésőbb három napon belül aktualizálja.
143. Az eszközökön (a számítógépeken, laptopokon és a mobil eszközökön) a kötelező biztonsági elemek (jelszó, időzáras képernyőzár stb.) beállítása (központi- vagy helyi szabályozással) az Informatikai Osztály feladata.
144. Az eszközök átadásának-átvételének megtörténte feltételezi a biztonsági elemek meglétét és a felhasználó tudomását ezen biztonsági elemek kötelező használatáról, így a felhasználó az eszközért és annak biztonságos használatáért teljes körű felelősséggel tartozik.
145. Az eszközök teljes életciklusa alatt kötelező azok nyilvántartása és mozgásuk dokumentálása (üzembe helyezési dokumentum, átadás-átvétel nyomtatvány, szállítók, selejtezési bizonylat). Az informatikai berendezéseket, eszközöket fizikai valójukban is védeni kell a biztonságot fenyegető veszélyektől és a káros környezeti hatásoktól.

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

147. Az informatikai eszközök rendeltetésszerű használatáért a számviteli leltárban az eszköz használójaként kijelölt alkalmazott a felelős, vagy az a személy, aki vezetői utasításra és engedéllyel azt használta. Közös használatú eszköz esetén az eszközök rendeltetésszerű használatáért az a személy felelős, akit a vezető adott esetben kijelölt az eszköz felügyeletére (csoportvezető, ügyeletes, munkafelelős stb.).

148. A munkája során számítógépet használó felhasználó köteles az általa működtetett számítógépet és az ahhoz csatlakoztatott eszközöket:
a) rendeltetésnek megfelelően, munkavégzés céljából, szakszerűen, a Főigazgatóság érdekeit szem előtt tartva jelen szabályzatban meghatározott módon használni,
b) kikapcsolni, amennyiben előre láthatóan hosszabb (3 órát meghaladó) ideig nem használja (pl. értekezlet, megbeszélés, tárgyalás).

149. Az informatikai eszközök használata során tilos:
a) az eszközt illetéktelen személynek átengedni,
b) az eszköz közelében folyadékot, éghető anyagot, és felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni, valamint
c) az eszközt a telepítési helyéről elmozdítani és elvinni a kijelölt informatikus engedélye és közreműködése nélkül (kivételt képeznek a mobil eszközök).

150. Az informatikai eszközökhöz bármilyen külső eszközt, illetve kábelt csatlakoztatni csak a kijelölt informatikus engedélyével vagy közreműködésével lehet. Az engedély kiadható egyszeri csatlakoztatásra vagy általános engedélyként. Az informatikus által már csatlakoztatott és beüzemelt eszköz további használata visszavonásig engedélyezett (pl. pendrive, fényképezőgép).

151. A Főigazgatóság területén az informatikai rendszert, áramellátó hálózatot, telefonhálózatot érintő bármilyen beavatkozást, építést, karbantartást, átalakítást csak az Informatikai Osztály, az igazgatóságok esetében az igazgató (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) tájékoztatása után, annak jóváhagyásával és felügyeletével lehet végezni.

152. A mobil informatikai eszközről az arra felhatalmazott személy részére történő átadásakor az Informatikai Osztály kijelölt informatikusa átadás-átvételi nyilatkozatot készít, ami tartalmazza az eszköz műszaki adatait, az átadás-átvétel adatait

153. A mobil eszközöket használó személyeknek:
a) kötelező a képernyőzár használata, melynek feloldása egyedi azonosítóval történhet (jelkód, számkód, ujjlenyomat, arcfelismerés) amennyiben a telefonon működő operációs rendszer rendelkezik erre alkalmas funkcióval (általános védelem),
b) nem engedélyezett az eszközt gépjárműben, idegen helyen felügyelet nélkül hagyni,
c) a repülés, vagy vonatút alatt a mobil informatikai eszközt kézipoggyászként kell szállítaniuk,
d) a Főigazgatóság területén kívül, idegen helyen történő tárolás esetén (szálloda, lakás) fokozott figyelmet kell fordítaniuk a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemre,
e) nem engedélyezett az eszköz engedély nélküli átruházása vagy adatainak közlése,
f) nem engedélyezett megfelelő védelem nélkül idegen hálózathoz csatlakoztatni az eszközt, [pl. jelszó nélkül elérhető vezeték nélküli (Wi-Fi) hálózatok],

g) a mobil eszköz átadása más felhasználó (vagy illetéktelen személy) részére tilos, ezzel ellenkező esetben a felhasználó teljes felelősséggel tartozik a Főigazgatósággal szemben,
h) nem engedélyezett az eszközt bármilyen indokolatlan veszélynek kitenni vagy nem rendeltetésszerűen használni.

154. A kódolatlan mobil adathordozó eszközök rendkívül nagy kockázati veszélyforrást jelentenek, ezért a felhasználók ezeket csak informatikai ellenőrzés mellett használhatják.

155. A kódolatlan mobil adattárolókon hivatali adatokat, információkat tartalmazó dokumentumok kizárólag olvasási és módosítási jelszóvédelemmel ellátva kerülhetnek tárolásra. A dokumentumok kódolásáért a felhasználó kizárólagosan felelős.

156. Amennyiben a Főigazgatóság hivatali használatra átadott adathordozót a felhasználó számára, úgy azon magánjellegű adatot tárolni kizárólag a hivatali adatoktól elkülönítve (külön mappában tárolva) engedélyezett. A hivatali adathordozón tárolt adatokért a felhasználó kizárólagos felelősséggel tartozik.

157. Magánjellegű adathordozót hivatali célra használni engedélyezett, azonban hivatali adatot, dokumentumot kizárólag jelszóval védve lehet tárolni.

Ebben az esetben kötelező a megnyitáshoz és a szerkesztéshez jelszót rendelni. Az adatok, dokumentumok jelszóval való védettségéért a felhasználó kizárólagos felelősséggel tartozik.

158. A Főigazgatóság informatikai rendszerébe kapcsolt munkaállomásokon csak olyan adathordozót lehet használni, arról adatokat beolvasni, amelyen előtte a rendszeresített és telepített víruskereső programmal vírusellenőrzést végeztek.

159. A mobil infokommunikációs eszközök, mobil adathordozók felhasználói felelősek az eszközön található adatok esetleges kiszivárgásáért, az eszköz elvesztéséért, eltűnéséért, megsérüléséért. A mobil infokommunikációs eszközök, mobil adathordozók eltűnése, ellopása esetén annak tényét a felhasználónak haladéktalanul jelentenie kell a szükséges intézkedések megtétele érdekében.

160. A felhasználók egyes feladatok elvégzése érdekében, a részükre biztosított, nyilvántartott és egyedi azonosítóval ellátott, hivatali tulajdonú mobil adathordozóra kimenthetik a feladatukhoz kapcsolódó állományaikat.

161. A megsemmisítésre kijelölt eszközöket és kellékanyagokat megsemmisítésig a használatban lévő eszközöktől elkülönítetten kell tárolni és kezelni figyelembe véve:

a) a veszélyes anyagok tárolására és a megsemmisítésre vonatkozó szabályokat (fizikai védelem, szállítás),
b) a leltározási és selejtezési szabályzat előírásait, és
c) az adatvédelem biztonsági követelményeit (hozzáférés elleni védelem).

162. Az olyan hivatali helyiségeket, ahol informatikai eszközökkel történik a munkavégzés, vagy informatikai eszközt tárolnak, zárral kell ellátni és a helyiséget távollét esetén vagyonvédelmi és biztonsági okokból zárva kell tartani.

163. Az informatikai berendezések végleges használaton kívül helyezése előtt gondoskodni kell az összes adat, szoftver visszaállíthatatlan eltávolításáról és felülírásáról, vagy a beépített adathordozó eltávolításáról (roncsolásáról) és megfelelő tárolásáról.

164. A külső személy által javításra, megsemmisítésre elszállított informatikai eszközökből el kell távolítani a beépített adathordozót, amennyiben ez nem megoldott, a külső személy arra felhatalmazott képviselője a külső személy nevében érvényes és joghatályos nyilatkozatot köteles tenni az adatvédelmi és titoktartási szabályok betartására vonatkozóan.

165. A központi szervezeti egység esetében az Informatikai Osztály, valamint a Vagyongazdálkodási és Üzemeltetési Főosztály vezetője, egyéb esetekben az igazgató és az Vagyongazdálkodási és Üzemeltetési Főosztály vezetője a hozzá tartozó igazgatóságon gondoskodik:

a) a szerverek működéséhez szükséges megfelelő fizikai környezet biztosításáról,

b) a megfelelő elektromos hálózat, villám és túlfeszültség, valamint érintésvédelmi berendezések meglétéről és működésének biztosításáról,
c) a behatolás elleni védelem és riasztórendszer kialakításáról (pl. beléptető rendszer, elektromos behatolás jelző, mozgásérzékelő, belső térvédelem),
d) a megfelelő tűzvédelmi rendszerről,
e) füstjelző és riasztó rendszer kialakításáról,
f) automata tűzoltó rendszer kialakításáról, vagy kézi tűzoltó készülékek (elektromos berendezések tüzének oltására alkalmas gázzal oltó készülék) elhelyezéséről.

166. Az informatikai objektumok közüzemi ellátását (áramellátás, fűtés, szellőzés, vízszolgáltatás stb.) a vonatkozó szabályzatok és hatósági előírások szerint kell biztosítani.
167. A szerverszobában vizesblokk kialakítása nem engedélyezett. A szerverszobát védeni kell szennyvíz, vagy esővíz bejutása ellen. A kialakítás során törekedni kell arra, hogy a szerverszoba felett vizesblokk ne helyezkedjen el.

8. A hálózat- és rendszerüzemeltetés biztonsága

168. A rendszer napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése és hiba esetén az eszközök javítása.
169. A rendszer üzemeltetését ellátó informatikusoknak ismerniük kell a Főigazgatóság rendszereszközeinek, operációs rendszereinek, adatbázisainak működését, az operációs és alkalmazói rendszerek hibaüzeneteit és a behatolás detektáló rendszerfigyelmeztető üzeneteit, és tudniuk kell alkalmazni a szükséges reagálásokat tartalmazó leírást.
170. A rendszer felügyelete a felhasználói programok és adatbázisok, a szerverek és alapszoftverek, valamint a hálózat működésének folyamatos figyelemmel kísérését kívánja meg. A felelős informatikai munkatársaknak rendszeresen el kell végezniük azokat a tevékenységeket, amelyek alapján meggyőződhetnek arról, hogy a rendszer üzemszerűen, normálisan működik.
171. A rendszer valamennyi hardver, és szoftver eleméről nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a szerverek, munkaállomások pontos és naprakész hardver konfigurációját, a működtető szoftverek egyedi beállításait és elhelyezkedését, és az értük felelős személy nevét.
172. Az alábbi naprakészen vezetendő nyilvántartásokat szükséges elkészíteni:
a) szoftvernyilvántartás,
b) jogosultság nyilvántartás, valamint
c) eszköz átadás-átvételi adatlap.

173. Szoftvert a számítógépre csak az Informatikai Osztály/NISZ munkatársai telepíthet, valamint a számítógépről csak az Informatikai Osztály/NISZ munkatársai távolíthatnak el.
174. A felhasználó a munkaállomás használata során a munkaállomásra telepített alkalmazásokat használhatja. A felhasználó új alkalmazások telepítését vagy a meglévő alkalmazásokat illető jogosultságváltozást a szervezeti egység vezetője engedélyével igényelhet. Az Informatikai Osztály, igazgatóságoknál az igazgató az Informatikai Osztály vezetőjével történő egyeztetés után (vagy az általa ezzel megbízott munkatárs) jogosult az igény felülvizsgálatára, és amennyiben szükséges, biztonsági okból annak elutasítására.
175. A felhasználó a számítógépre telepített alkalmazásokat a felhasználói leírás szerinti módon, szakszerűen köteles használni.
176. Tilos a szoftvereket és adatokat harmadik fél számára másolni, és továbbadni.
177. 176. pontban foglaltak alól kivételt képez a szoftverekről és adatokról való biztonsági másolatok kijelölt informatikus által történő elkészítése, amely a rendelkezésre állás folyamatosságát hivatott biztosítani.

178. A szoftverek adathordozóit, üzemeltetési és felhasználói dokumentációját, licenc dokumentációját az Informatikai Osztály, a NISZ által biztosított gépekre telepített szoftverekről, a NISZ által megbízott munkatárs tárolja és tartja nyilván.
179. A hibabejelentéseket a kijelölt informatikusok személyes, telefonos megkeresésével és vele párhuzamosan e-mailben lehet elvégezni.
180. A felhasználó által észlelt hardver/szoftver hiba esetén köteles az Informatikai osztály felé jeleznie a hibát, a kijelölt informatikus feladata, hogy saját eszköz (TEF tulajdon) esetén gondoskodjon a szükséges hibaelhárításról, az eszköz javításáról, az eszköz helyettesítéséről, az eszköz szervizbe szállításáról, a NISZ által üzemeltetett eszköz esetén jelezze a hibát írásban a NISZ ügyfélszolgálat felé.
181. A kijelölt informatikus feladata, hogy tájékoztassa az érintett felhasználót az eszköz javítási folyamatáról és sorsáról.
182. Abban az esetben, amennyiben a hiba a Főigazgatóság rendszereinek működésére komoly kihatással van (pl. üzembiztonságot veszélyeztető helyzet, katasztrófahelyzet áll fenn), vagy más jellegű, azonban rendkívül fontos eset következik be (pl. bűncselekmény gyanúja áll fenn), az észlelő köteles haladéktalanul értesíteni az Informatikai Osztály munkatársát.
183. A külső üzemeltetői erőforrások (harmadik fél) bevonása esetén pontosan meg kell határozni a feladatok és a felelősségek megosztását, jelen szabályzatban meghatározott biztonsági követelmények rögzítése mellett.
184. A hálózati végpontok és az azokra csatlakoztatott eszközök végpontvédelméről minden informatikai eszköz esetében gondoskodni kell. A védelem során gondoskodni kell, hogy:

a) illetéktelenek ne férjenek szabadon maradt hálózati végpontokhoz,
b) illetéktelenek ne csatlakozhassanak a hálózatához (ne kapjanak hálózati azonosítót a hálózati erőforrások eléréséhez),
c) illetéktelenek ne léphessenek be a számítógépekbe, valamint
d) ne legyen támadható vezeték nélküli vagy vezetékes kapcsolat a rendszerben.

185. A Főigazgatóság épületeiben hálózati végpontot csak ellenőrzött körülmények között lehet létesíteni.
186. Minden olyan asztali vagy hordozható számítógépet, mobiltelefont végpont védelemmel kell ellátni, ami alkalmas:

a) a hálózathoz csatlakozásra,
b) az adatok kimásolására és továbbítására,
c) USB adathordozó eszköz csatlakozásra, valamint
d) vezeték nélküli kapcsolatok létesítésére.

187. A vírusvédelmi rendszert a Főigazgatóság minden számítógépére telepíteni kell.
188. Tilos olyan eszközt az informatikai hálózathoz csatlakoztatni, amelyre nincs telepítve vírusvédelem, ha az eszközről a rendszerek bármelyikét, a bennük lévő adatállományokat eléri.
189. A végpontvédelmi intézkedések nem akadályozhatják az alapvető működési feladatokat, ezért biztosítani kell a munka során használt engedélyezett (nyilvántartott) és a feladat végrehajtásához szükséges eszközök (nyomtató, szkenner stb.) zavartalan működését.
190. A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az üzemeltetett rendszerek előre nem látható esemény (katasztrófa vagy hardver, szoftver meghibásodása, emberi mulasztás) bekövetkezte után, szükség esetén rövid időn belül helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell, hogy az üzemidő-kiesés, adatsérülés, adatvesztés kockázata minimális legyen.
191. A mentés ütemezését mentési egységenként lehetőleg úgy kell kialakítani, hogy a mentés a munkafolyamatokat, és a munkafolyamatok a mentési eljárást ne akadályozzák.
192. A biztonsági mentés a napi adatbiztonságot szolgáló rendszeresen készülő mentésfajta (szerveren vagy munkaállomáson), amely biztosítja a napi munka során felmerülő kisebb

meghibásodásokból származó adatvesztések, adatbázis-konzisztenciahibák megszüntetését a lehető legkisebb időráfordítással. Előbbi esetben a mentés:

a) egy (azonos tűzszakaszban elhelyezett) másik szerverre,
b) az adott szerverbe beépített tartalék HDD-re, vagy
c) a szerverhez kapcsolt külső HDD-re valósul meg.

193. A mentést követően ellenőrizni szükséges a mentésről készített digitális naplót vagy meg kell győződni a mentés megtörténtéről. A biztonsági mentés használata mellett biztosítani kell egy tűzvédelmi mentést is.

194. A tűzvédelmi mentés a napi adatbiztonságot szolgáló rendszeresen készülő mentésfajta (szerveren vagy munkaállomáson), amely biztosítja a súlyosabb meghibásodásokból származó (katasztrófa, hardver vagy szoftver meghibásodás esetén történő) rendszerösszeomlások, adatvesztések, adatbázis-konzisztenciahibák megszüntetését a lehető legkisebb időráfordítással.

195. A tűzvédelmi mentés történhet egy másik szerverre, amennyiben az nem azonos tűzszakaszban található a mentett eszközzel (hálózaton keresztül történő mentés), amelynek használata esetén a következőket kell biztosítani:

a) a munkanap kezdetén az előző napi mentés sikerességét ellenőrizni kell,
b) amennyiben a mentés adathordozóra történik, akkor biztosítani kell:
   ba) a mentési adathordozók rendszeres váltott cseréjét,
   bb) figyelemmel kell lenni az adathordozók felhasználhatóságának paramétereire (pl. hányszor írható),
   bc) az adathordozók előírás szerinti tárolását.

196. Egyedi mentéssel kell biztosítani azon munkaállomások és mobil eszközök háttértárolóin keletkezett alkalmazások és felhasználói állományok mentését, amelyekről

a) nem történik rendszeres napi mentés a hálózatra, vagy
b) az eszközzel kapcsolatban egyedi mentési igény merül fel,
c) azon hálózati közös meghajtók rendkívüli mentését, amelyre vonatkozó igény a tárkapacitás túlterheltsége miatt merült fel.

197. A hálózaton tárolt telepítő készletek és programok mentéséről folyamatosan gondoskodni kell.

198. A mobil adathordozó eszközök (pl. pendrive, külső HDD) kiadása, állapotváltozása, visszavétele az Informatikai Osztály kijelölt informatikusának feladata.

199. A mentés elkészítéséhez használt adathordozó típusok kiválasztásánál az alábbiakat kell figyelembe venni:

a) a mentendő adatmennyiségnek megfelelő tárolókapacitás,
b) a megfelelő adatmegőrzési idő (legalább 5 év különleges beavatkozás, speciális eljárások alkalmazása nélkül),
c) megfelelő ellenállás a környezeti viszonyoknak (hőmérséklet, páratartalom, fény stb.),
d) adat-visszaállítás esetére szükséges eljárások és eszközök rendelkezésre állása.

200. A Főigazgatóság elektronikus szoftvereinek telepítőkészletei vagy adatainak mentésére és archiválására használt adathordozói, a mentés dokumentuma, a helyreállítást biztosító leírások:

a) biztonságos módon, a mentés helyétől (telepítés helyétől) különböző helyen elhelyezett tűzbiztos fémszekrényben,
b) a mentés helyétől (telepítés helyétől) különböző tűzszakaszban elhelyezkedő helyiségben tárolandók és az elhelyezésükre,
   ba) megfelelő mechanikai védelemmel rendelkező (pl. ablakráccsal, biztonsági zárral),
   bb) elektronikus védelemmel (riasztórendszerbe integrált, füst-, illetve hő-érzékelővel) ellátott,
   bc) lehetőleg regisztrált kulcsfelvétellel hozzáférhető, és
   bd) közművezetékektől mentes
   helyiséget kell kijelölni.

201. A mobil adathordozó eszközöket nyilván kell tartani.
202. Az operációs rendszerek, programok, eszközkezelők telepítő állományait tartalmazó adathordozókról nyilvántartást kell vezetni, amely történhet digitális formában, illetve az informatikai nyilvántartás keretében.

9. Elektronikus információs rendszerek

203. A Főigazgatóság által használt központi információs rendszerek:
a) Központi adattároló rendszer (File Szerver),
b) Integrált gazdasági rendszer (Forrás SQL, KIRA),
c) Ügyviteli és iktatási rendszer (Robotzsaru),
d) Humánpolitikai rendszer (SZENYOR),
e) Lokális Dokumentumok mappa,
f) Főigazgatóság weboldala,
g) Képzési rendszer (KIR),
204. Annak érdekében, hogy a 2013. évi L. törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.
205. Az elektronikus információs rendszerek biztonsági osztályba történő besorolása az informatikai biztonsági referens feladata, amelyet a szervezeti egységekkel, és az információs rendszerek szállítóival, fejlesztőivel közreműködve végez el.
206. Az elektronikus információs rendszerek biztonsági besorolása után meg kell vizsgálni, hogy a rendszerekben, valamint annak informatikai környezetében milyen megoldások, biztonsági intézkedések kerültek megvalósításra, s ezek milyen hatékonysággal működnek. Ezen vizsgálat eredményeképpen meghatározásra kerülnek az elektronikus informatikai rendszerek jelenlegi biztonsági szintje.
207. Amennyiben az információs rendszerek jelenlegi biztonsági szintje nem éri el a 206. pontban kialakított, azaz a kívánt biztonsági szintjét, úgy az informatikai biztonsági referens cselekvési (intézkedési) tervet készít a megfelelő biztonsági szint eléréséhez, figyelemmel a törvényben megszabott szintlépések közötti határidőre is.
208. Az informatikai biztonsági referens a biztonsági osztályba sorolást a törvényben előírt időszakonként, azaz legalább háromévente, vagy szükség esetén soron kívül felülvizsgálja.

10. A rendszerek hozzáférési jogosultságainak kezelése

209. A szervezeti egység vezetője írásban köteles tájékoztatni az Informatikai Osztályt, a szervezeti egységnél, az igazgatóságon a felhasználókra vonatkozó minden változásról (felvétel, kilépés), amely az informatikai vagy kommunikációs rendszert érinti. A szervezeti egység vezetője jogviszonyának megszűnésekor a munkáltatói jogkör gyakorlója gondoskodik a jogosultságok töröltetéséről.
210. A felhasználói jogosultságok igénylése és kiosztása esetében törekedni kell arra, hogy egy felhasználó csak a munkavégzéshez szükséges és elégséges legszűkebb jogosultságokkal rendelkezzen. A túl széles jogosultsági kör a Főigazgatóság adatintegritásának veszélyeztetésével jár, amelyért a felhasználónak jogosultságokat igénylő szervezeti egység vezetője teljes felelősséggel tartozik.
211. A Főigazgatóság minden felhasználója a belépésekor az alábbi jogosultságokkal és hozzáférésekkel rendelkezik alapértelmezetten:

a) Felhasználói azonosító,
b) elektronikus levelezési cím,
c) a dokumentumkezelő- és iktatórendszerben alkalmazotti szerepkörrel,
d) FileServer jogosultság.

212. A vezető beosztású felhasználók a fentieken felül rendelkeznek a Robotzsaru vezetői felületének jogosultságával.

213. Jogosultságok igénylésének, módosításának, megszüntetésének céljából belső használatra létrehozott igénylőlap használata rendszeresített, amelynek kötelező tartalmi elemei a következők:

a) Új igény (új belépő) esetén:
   aa) a belépő adatai (név, szervezeti egység, beosztás, munkavégzés helye),
   ab) eszközigénylés [számítógép, laptop, mobiltelefon , SIM kártya
   ac) az alapértelmezetten járó jogosultságok és hozzáférések részletezése,
   ad) az elérhető informatikai rendszerekhez való hozzáférés igénylése, amennyiben részletezhető, akkor a hozzáférés szintjének megadása (pl. szerepkör vagy modulok megjelölésével). Amennyiben a megjelölt informatikai rendszert nem az Informatikai Osztály kezeli, az igényt írásban (akár elektronikus levél formájában) jelezni kell az illetékes szervezeti egység felé,
   ae) az igényt az új felhasználó szervezeti egységének vezetője hitelesíti.
   b) Robotzsaru ügykezelő és iktató rendszer jogosultságainak igénylése
   ba) Igénylő adatai,
   bb) szerepkörei,
   bc) iktatókönyvei.
c) Felhasználói jogosultságok és hozzáférések megszüntetése (felhasználó kilépése vagy hosszabb távollét) esetén:
   ca) a kilépő felhasználó elektronikus levelezési postafiókjával kapcsolatos teendők,
   cb) a postafiók archiválásának igénye,
   cc) a postafiók megszüntetésének időpontja,
   cd) a postafiók megszüntetéséig mely felhasználóknak legyen betekintési jogosultságuk a kilépő felhasználó postafiókjának Beérkezett Üzenetek mappájára,
   ce) a kilépő felhasználó számítógép adatai archiválásának kérése,
   cf) a számítógép visszaadásáról történő döntés az Informatikai Osztály részére írásban vagy a NISZ felé az ügyfélszolgálaton keresztül.
d) A felhasználó szervezeti egység váltása esetén:
   da) a felhasználó adatai (név, régi szervezeti egysége, régi beosztása, új szervezeti egysége, beosztása),
   db) a régi szervezeti egység vezetőjének rendelkezései,
   dc) az elektronikus levelezéssel kapcsolatos kérdések,
   dd) a felhasználói postafiók archiválásának kérése,
   de) az archivált adatok mely felhasználók részére kerüljenek átadásra/beállításra,
   df) az adatoknak a felhasználói postafiókból törléséről való rendelkezés (kéri vagy nem kéri),
   dg) a felhasználó számítógépével kapcsolatos kérdések,
   dh) az adatok archiválásának elrendelése,
   di) a számítógép átadása (az új szervezeti egységnek, az Informatikai Osztálynak, átadás megtagadása),
   dj) az új szervezeti egység vezetőjének rendelkezései,
   dk) az új szervezeti egységhez tartozó terjesztési lista tagság és a technikai fiókhoz való előre meghatározott hozzáférési szint automatikusan beállításra történik (tájékoztató),

dl) a dokumentumkezelő- és iktatórendszerben a felhasználó az új szervezeti egységhez kerül hozzárendelésre automatikusan (tájékoztató),
dm) egyéb terjesztési lista tagság kérése,
dn) egyéb technikai fiókhoz való hozzáférés kérdése (hozzáférési szint megadásával),
do) elérhető informatikai rendszerekhez való hozzáférés igénylése (, amennyiben részletezhető, akkor a hozzáférés szintjének megadása),
dp) a szervezetváltási kérelmet mindkét szervezeti egység vezetőjének aláírása hitelesíti, a főosztályvezetői, vagy szervezeti igazgató beosztásokat érintő szervezeti egység váltás esetén a főigazgató aláírása hitelesíti a kérelmet.

e) Egy informatikai rendszerhez már működő hozzáférés szintjének módosítása, vagy megszüntetése esetén elegendő a hozzáférést igénylő felhasználó közvetlen vezetőjének elektronikus bejelentése (Robotzsaru rendszer – jogosultság változás

214. A felhasználóval kapcsolatban felmerülő alábbi informatikai igényeket írásban kell jelezni az Informatikai Osztálynak, budapesti telephelyek esetén a NISZ felé:

a) informatikai eszközigénylés, mozgatás, áthelyezés és átvezetés,
b) informatikai rendszerhez hozzáférés-változtatási igény (igénylés, módosítás vagy törlés),
c) alkalmazástelepítési vagy -eltávolítási igény,
d) inaktívvá válás esetén újraaktiválás kérése,
e) munkavégzési hely vagy feladat változása esetén egyedi vagy tömeges eszközmozgatási és telepítési igény,
f) hálózattal kapcsolatos igény (kiépítés, bővítés, elbontás),
g) informatikai szolgáltatáshoz, alkalmazáshoz, hálózati mappához (könyvtár) való hozzáférés, valamint ezekkel kapcsolatos jogosultság változása (igénylés, módosítás vagy törlés).

215. Az írásban bejelentett igény alapján az Informatikai Osztály kijelölt informatikusa elvégzi vagy külső fél (NISZ) által szolgáltatott rendszer esetén elvégezteti az informatikai rendszerben:

a) az adatok átvezetését, a szükséges beállításokat,
b) letiltja vagy engedélyezi az informatikai szolgáltatásokat (pl. levelezés, internet, hálózati mappa elérése, nyomtatás stb.),
c) elvégzi a jogosultságok nyilvántartását, amennyiben az adott rendszerből az informatikus által lekérdezhető, akkor a jogosultságok rendszerben történő átvezetésével, egyéb esetben külön (elektronikus vagy papíralapú) jogosultsági nyilvántartás vezetésével,
d) a kijelölt informatikus átadja, átveszi, átvezeti, beállítja, és törli az informatikai eszközöket és jogokat a belépő, kilépő, meglévő felhasználóknak,
e) elvégzi az informatikai eszközök nyilvántartására vonatkozó teendőket,
f) kilépő dolgozó vagy munkakör változása esetén elvégzi és a szervezet vezetője, és a Humánpolitikai Osztály felé igazolja a nyilvántartás szerint a dolgozó nevén lévő eszközök átvezetését, valamint jogosultságainak kivezetését a rendszerből.

216. A Főigazgatóság informatikai rendszerét úgy kell kialakítani és olyan szoftvereket szabad használni, hogy a rendszerbe felhasználó csak hitelesítés (a felhasználónév és a jelszó megadása) után jelentkezhessen be.

217. A Főigazgatóság által használt (Saját tulajdonú) informatikai eszközökön adminisztrátori jogosultsággal kizárólag az Informatikai Osztály dolgozói rendelkezhetnek, minden felhasználó kizárólag felhasználói joggal rendelkezhet, ettől eltérés csak az Informatikai Osztályvezető írásos engedélyével alapján történhet.

218. A Főigazgatóság budapesti telephelyein a munkatársak hálózatba kapcsolt számítógépeit a NISZ biztosítja, az EI rendszerbe kapcsolt eszközökre adminisztrátori joggal kizárólag a NISZ rendelkezik.

219. Az informatikai eszközöket, amennyiben a hozzáférhetőség vagy a fontosság miatt indokolt (számítógép, nyomtató, multifunkciós eszköz, switch stb.), és amennyiben az eszköz operációs rendszere megengedi, valamint a hálózathoz való hozzáférést minden esetben felhasználói azonosítóval (felhasználói név és jelszó) kell védeni.
220. Az adminisztrátori jogokat személyi vagy munkaköri változás esetén, vagy legalább évente felül kell vizsgálni.
221. A nem használt (tartalék, javításra váró vagy javításból érkezett) informatikai eszközök tárolásáról az Informatikai Osztály gondoskodik.

11. Biztonsági kockázatmenedzsment

222. A Főigazgatóság információ biztonsági referense évente egyszer a rendelkezésre álló információk alapján (amelyet a szervezeti egységek írásban bocsátanak rendelkezésre) kockázatelemzést köteles készíteni.
223. A kockázatelemzés során az egyes veszélyforrások által képviselt kockázatokat kell megállapítani és feltárni. A kockázat meghatározása a veszély megvalósulásának valószínűsége és az okozható kár alapján vagy más nézőpontból, az adott veszélyt képviselő sérülékenység kihasználhatósága és ennek hatása alapján történik.
224. A Főigazgatóság információ biztonsági referense elemzés során a kockázatokat kategóriákba sorolja, értékeli.
225. A kockázatelemzésről szóló jelentés alapján az Informatikai Osztály vezetője elkészíti a kockázatok csökkentését célzó intézkedési tervet az informatikai biztonsági referens közreműködésével. Az informatikai biztonsági referens feladata az intézkedési terv határidejének és a benne foglalt intézkedések végrehajtásának ellenőrzése, amelyről írásos tájékoztatást ad a főigazgatónak.
226. A kockázatkezelés lépései:
a) a kockázatok feltárása, csoportosítása és hatáselemzése,
b) a szükséges lépések, módszerek meghatározása és hatáselemzés,
c) megoldási tervek és alternatívák készítése,
d) döntés és megvalósítás,
e) monitoring és utóellenőrzés.
227. A kockázatkezelés szabályai:
a) a valós kockázatokat kell figyelembe venni,
b) minden körülményt figyelembe kell venni,
c) a súlyosság mértéke szerint kell haladni a kockázat megoldása és elhárítása során,
d) a megoldások közül azt a módszert (eszközt kell választani), amelyik a legnagyobb eredményt hozza a legkisebb erőforrás ráfordítással,
e) a kockázatkezelésre fordított erőforrások, a védekezés költségei arányosak kell, hogy legyenek a kockázat mértékével.

12. Ellenőrzés

228. Az IT-biztonság kontrollja az alábbi eszközökkel biztosítható:
a) dokumentált eszközkezelés (üzembe helyezési, eszközátadási, eszközszállítási, leltározási és selejtezési események dokumentálása),
b) a jogosultságok és hozzáférések dokumentálása,
c) ellenőrzött szoftverkezelés (jogtisztaság, tesztelt szoftverek, szoftvernyilvántartás vezetése, telepítés jogosultság szabályozása),
d) mentések és archívumok készítésére, valamint tárolására vonatkozó előírások és kapcsolódó nyilvántartások vezetése,

e) a munkahelyek, hálózatok, informatikai helyiségek kialakítására és üzemeltetésére vonatkozó előírások betartása, kapcsolódó események naplózása,
f) hibakezelési rendszer alkalmazása és ellenőrzése, elemzése, valamint
g) az IT biztonsági többszintű ellenőrzése.

229. Az információ biztonsági referens az éves ellenőrzések során szúrópróbaszerűen ellenőrzi az IT-biztonsági dokumentumokat és jelentés formájában az Informatikai Osztály vezetőjét tájékoztatja.
230. Az IT-ellenőrzések területei:
a) környezeti veszélyek – pl. természeti károk, tűz, stb.,
b) fizikai veszélyek – lopás, rongálás, betörés,
c) informatikai veszélyek – vírusok, számítógépes betörés, stb.,
d) humán veszélyek – szabotázs, gondatlanság, tudatlanság, felelőtlenség, stb.,
e) szervezeti veszélyek – szervezeti problémák, irányítási gondok, stb.
231. Az IT-ellenőrzések rendszere a Főigazgatóságnál:
a) alapszintű ellenőrzés: az Informatikai Osztály informatikusai által,
b) középszintű ellenőrzés:
ba) a szervezeti egység vezetőinek személyes részvételével,
bb) az Informatikai Osztály vezetője, vagy az informatikai biztonsági referens ellenőrzései,
bc) a Belső Ellenőrzési Osztály ellenőrzései,
c) felsőszintű ellenőrzés: központi szakmai irányító szervek, hatóságok ellenőrzései felügyeleti kontrollja, és ellenőrzése.

13. Átmeneti és záró rendelkezések

232. Jelen szabályzatban előírtak alapján utólagosan el kell készíteni a szükséges nyilvántartásokat, ami – figyelemmel a nagy tömegű utólagos adatgyűjtésre és manuális munkára – a szabályzat hatályba lépésétől számított 6 hónapon belül történik meg.
233. Az elkészítendő nyilvántartások:
a) tárolási nyilatkozat: elkészítendő az összes, jelenleg felhasználónál található mobil eszközre,
b) szoftvernyilvántartás: elkészítendő az összes, jelenleg érvényes és alkalmazott szoftver telepítőkészletére, valamint
c) jogosultság nyilvántartás: elkészítendő az összes, jelenlegi felhasználó minden olyan jogosultságára, ami a rendszerekből nem kérdezhető le (ezt a későbbiekben a szerepkörök megalkotása és a jogosultságok részletes leírása vagy hozzárendelése válthatja ki).
234. Az informatikai helyiségek fizikai környezetének kialakítására vonatkozó előírásoknak való megfelelést meg kell vizsgálni. Megfelelőségének hiányában intézkedési tervet kell készíteni jelen szabályzat hatályba lépésétől számított 6 hónapon belül.
235. A mentések technikai, műszaki hátterének meglétét, a tűzvédelmi terveket meg kell vizsgálni. Előbbiek megfelelőségének hiányában intézkedési tervet kell készíteni a szabályzat hatályba lépésétől számított 6 hónapon belül.
236. A felhasználók informatikai eszközökkel való ellátottságát, a saját tulajdonú eszközök (pl. pendrive, notebook) hivatali célra történő használatát meg kell vizsgálni. Előbbiek megfelelőségének hiányában intézkedési tervet kell készíteni jelen szabályzat hatályba lépésétől számított 6 hónapon belül.

237. A mobil adathordozók használatára vonatkozó szabályokat felül kell vizsgálni. A vizsgálat határideje 2020. június 30. A vizsgálatot az Informatikai Osztály és az informatikai biztonsági referens együtt végzi.
238. Az elektronikus informatikai rendszerek nyilvántartását és a rendszerek biztonsági szintbe való besorolását (az elvárt és a jelenlegi biztonsági állapot leírását) és a hozzá kapcsolódó cselekvési tervet (intézkedési tervet) el kell készíteni, amely az Informatikai Osztályának, azon belül is az informatikai biztonsági referens feladata, amelynek határideje 2020. június 30.
239. Az elektronikus informatikai rendszerek biztonsági szint besorolásának felülvizsgálati határideje 2020. július 01. A feladatot az informatikai biztonsági referens végzi, bevonva a rendszert használó és abban adatot, információt tároló szakmai szervezeti egységeket.
240. Az informatika rendszerek üzemeltetéséhez új dokumentációs szabályok, eljárások kialakítása szükséges. A részletszabályok kidolgozásának határideje 2020. december 31. A részletszabályokat az Informatikai Osztály és az informatikai biztonsági referens végzi.
241. Jelen szabályzat ellenőrzésére eljárásrendet kell kialakítani, amely az Informatikai Osztálynak feladata, kialakításának határideje a szabályzat hatályba lépésétől számított 6 hónap.

14. Záró rendelkezések

242. Ez a szabályzat az aláírás napját követő napon lép hatályba.

Budapest, 2020. 2020 MÁJ 05.

Sztojka Attila
főigazgató