9/2020.

A Nemzeti Kommunikációs Hivatal
Informatikai Biztonsági Szabályzata

Hatályba lépés dátuma: 2020. szeptember 11

Budapest, 2020. szeptember 10.

A szabályzatot kiadta: Dr. Lenkei Mirtill elnök

A Nemzeti Kommunikációs Hivatal Elnökének

9./2020. (..IX.10..) NKOH utasítása

a Nemzeti Kommunikációs Hivatal

Informatikai Biztonsági Szabályzatáról szóló 22/2017. (XII. 7.) NKOH utasítás módosításáról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés *c)* pontjában foglalt felhatalmazás alapján, figyelemmel az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet alapján a Nemzeti Kommunikációs Hivatal információs biztonságának szabályozása érdekében a következő utasítást adom ki:

1. A Nemzeti Kommunikációs Hivatal Informatikai Biztonsági Szabályzatáról szóló 22/2017. (XII. 7.) NKOH utasítás Melléklete helyébe a Melléklet lép.

2. Ez az utasítás 2020. 09. 11. napján lép hatályba.

Budapest, 2020. napja szeptember 10.

NEMZETI KOMMUNIKÁCIÓS HIVATAL * 1. *

dr. Lenkei Mirtill

elnök

I. ÁLTALÁNOS RENDELKEZÉSEK

1. §

(1) A Nemzeti Kommunikációs Hivatal (a továbbiakban: NKOH) Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) személyi hatálya kiterjed:

a) a Hivatallal a kormányzati igazgatásról szóló 2018. évi CXXV. törvény (a továbbiakban: Kit.) szerinti kormányzati szolgálati jogviszonyban álló valamennyi kormánytisztviselőre,

b) a Kit. 279. §-a alapján a Hivatallal munkaviszonyban álló munkavállalóra, valamint

c) az NKOH-val foglakoztatási jogviszonyban álló valamennyi munkavállalóra (a továbbiakban a)–c) pont együtt: munkatárs).

(2) Minden munkatárs köteles az IBSZ-ben felsorolt folyamatokat, ajánlásokat, szabályozásokat megismerni, betartani és azt másokkal is betartatni.

(3) Az IBSZ hatálya kiterjed azon, az NKOH-val szerződéses jogviszonyban álló természetes és jogi személyekre (a továbbiakban: szerződéses partner), akik bármilyen módon kapcsolatba kerülnek az NKOH informatikai infrastruktúrájával, vagy bármely, az IBSZ hatálya alá tartozó, a megbízható működést vagy információ védelmet érintő összes eszközzel, a velük kötött szerződésben és titoktartási megállapodásban szabályozott mértékben.

(4) Az IBSZ tárgyi hatálya kiterjed:

a) az NKOH informatikai rendszereire,

b) az informatikai rendszerekben feldolgozás alatt álló és ott tárolt, illetve a feldolgozás eredményeként létrejött minden iratra, adatra és adathordozóra, függetlenül annak feldolgozási, vagy előállítási módjától és megjelenési formájától,

c) az informatikai alkalmazás teljes életciklusára,

d) alkalmazási programok és azok dokumentációinak tervezési, fejlesztési, megvalósítási és működési szakaszaira,

e) az informatikai berendezések üzemeltetéséhez szükséges alap- és rendszerprogramok megvalósítási és működési szakaszaira, adathordozók tárolására és felhasználására,

f) az NKOH területén kívül tárolt eszközökre, adatokra.

(5) Az IBSZ területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai erőforrások üzemelési helyszíneire.

2. §

Vonatkozó jogforrások

(1) Az IBSZ-ben nem szabályozott kérdésekben

a) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.),

b) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,

c) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: 41/2015. BM rendelet),

d) a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011. (XII. 31.) Korm. rendelet (a továbbiakban: Bkr.),

e) a Nemzeti Kommunikációs Hivatalról és a kormányzati kommunikációs beszerzések központosított közbeszerzési rendszeréről szóló 247/2014. (X. 1.) Korm. rendelet (a továbbiakban: 247/2014. Korm. rendelet),

f) Nemzeti Kommunikációs Hivatal Szervezeti és Működési Szabályzatáról szóló 1/2019. (II. 21.) MK utasítást (a továbbiakban: NKOH SZMSZ),

g) az NKOH/ 652-1 (2016) iktatószámú, az NKOH és az MK között 2016. június 8-án létrejött, 2017. június 29-én módosított munkamegosztási megállapodás, valamint

h) az NKOH elnökének utasításait

kell alkalmazni.

3. §

Kötelező felülvizsgálat rendje

(1) Az IBSZ, valamint függelékei felülvizsgálatára az alábbiak szerint kerül sor:

a) évente egy alkalommal, a belső felülvizsgálatok során,

b) minden olyan esetben, amikor az IBSZ-ben leírtakhoz képest jelentős változás történik,

c) az eredeti szabályozás alapjait érintő minden változás (új kockázatok, új káresemények, új veszélyhelyzetek, és a műszaki infrastruktúra átalakítása) esetén soron kívül.

(2) A mindenkori felülvizsgálat végrehajtása az IBSZ-ben meghatározott informatikai biztonsági felelős (a továbbiakban: IBF) feladata az NKOH érintett munkatársainak közreműködésével.

II. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

4. §

Szervezeti szintű alapfeladatok

(1) Az NKOH az informatikai biztonsági irányítási rendszer bevezetése és fenntartása érdekében:

a) meghatározza az irányítási rendszer működtetéséhez szükséges információbiztonsági folyamatokat,

b) meghatározza a folyamatok hatásos működéséhez, szabályozásához szükséges kritériumokat és módszereket,

c) gondoskodik a folyamatok működéséhez és figyelemmel kíséréséhez szükséges erőforrásokról,

d) kockázatértékeléssel megállapítja az eszközeire, információ vagyonára irányuló fenyegetéseket, gyengeségeket, sebezhetőségeket és a szervezetre gyakorolt hatásokat, valamint meghatározza a kockázat mértékét,

e) a kockázatok, incidensek kezeléséhez meghatározza a fontossági sorrendet, a feladatokat és a felelősségeket,

f) a szabályozók (jogszabályi és szabványi követelmények) teljesítését figyelemmel kíséri, időszakonként felülvizsgálja, ellenőrzi.

(2) Az elvégzett kockázatértékelés módszerét, az informatikai biztonsági szintek és területek meghatározását jelen IBSZ és az Adminisztratív védelmi intézkedések eljárásrend elnöki utasítás tartalmazza.

5. §

Információbiztonsági politika

(1) Az NKOH elkötelezett az informatikai biztonság megvalósításában az alábbiak szerint:

a) meghatározza a biztonsági célokat, felállítja az információbiztonsági politika szervezeti szempontú alapelveit;

b) az informatikai biztonsági stratégia által bemutatja az NKOH elkötelezettségét a biztonsági feladatok irányítására és támogatására;

c) jelen IBSZ-ben kifejti az NKOH által alkalmazott biztonsági alapelveket és megfelelőségi követelményeket.

(2) Integrált kockázatelemzést és értékelést az NKOH évente, illetve tevékenységének ellátása során folyamataiban, infrastruktúrájában bekövetkező lényeges változások vagy új kockázatok, védendő értékek megjelenése esetén felülvizsgálja, ezáltal biztosítva, hogy megőrizze naprakészségét.

6. §

Az NKOH informatikai biztonsági szintje

(1) Az NKOH informatikai biztonsági szintje a 41/2015. BM rendelet 2. mellékletében foglaltak szerinti 3-as osztályba sorolt.

7. §

Informatikai biztonság szervezete

(1) Az informatikai biztonsági felelősségek az NKOH gyakorlatában kapcsolódnak a feladatok végrehajtásához. Ennek megfelelően az egyes tevékenységi területekhez, feladatteljesítésekhez kapcsolódó felelősségi körök az ügyrendekben, a szabályzatokban, belső utasításokban, vállalkozási és megbízási szerződésekben rögzítésre kerültek.

(2) Az informatikai biztonság megvalósítását az NKOH elnökének ellenőrzése mellett az IBF irányítja és felügyeli.

(3) Az IBF egyéb felelősségi körétől függetlenül biztosítja az Ibtv.-ben meghatározott elektronikus információs rendszerek védelméhez kapcsolódó feladatok ellátását, melynek keretében az IBF:

a) gondoskodik az NKOH elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az információbiztonsági tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) aktualizálja a jelen IBSZ-t,

d) aktualizálja az NKOH elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából az NKOH e tárgykört érintő szabályzatait és szerződéseit,

f) kapcsolatot tart a Nemzeti Elektronikus Információbiztonsági Hatósággal (a továbbiakban: hatóság).

(4) A felelősségek kijelölése biztosítja, hogy:

a) az informatikai biztonsági célkitűzéseket azok valósítják meg, akik felelősek a munka elvégzéséért,

b) a megfelelőség ellenőrzését azok végzik, akik nem közvetlenül felelősek a munka elvégzéséért,

c) a biztonsági auditok lebonyolítását a felülvizsgált területtől független személy végzi.

8. §

Cselekvési és intézkedési terv

(1) Az NKOH cselekvési terve az NKOH elnöke, az IBF és az üzemeltető által azonosított koncepcionális hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányul.

(2) A cselekvési tervben haladéktalanul rögzíteni kell:

a) a rendszerben a biztonsági osztály meghatározásánál és az ezzel kapcsolatban folytatott vizsgálatok során megállapított hiányosságok javítására hozott intézkedéseket,

b) a biztonsági osztály elérésével kapcsolatos hiányosságok, kockázatok feltárására évente tartott biztonsági auditok során feltárt problémák és az ezekre kidolgozott, csökkentésre vagy megszüntetésre irányuló eljárásokat.

c) A cselekvési terv a rendszerbiztonsági tervvel együtt frissítendő, az előírt tartalmat az IBF felelőssége bevezetni és karbantartani.

(3) Az IBF intézkedési tervet készít az alábbiak szerint:

a) a rendszerben azonosított sérülékenységek csökkentésére vagy megszüntetésére irányuló intézkedések végrehajtására,

b) amennyiben a (2) bekezdés szükségessé teszi,

c) jelen IBSZ-ben megfogalmazottak megvalósításához.

(4) Az intézkedési terv célja, hogy meghatározza az informatikai biztonság megvalósításához elvégzendő feladatokat, a feladatok elvégzésnek felelőseit és határidejét.

(5) Az IBF legalább évente felülvizsgálja és karbantartja az intézkedési tervet:

a) az Integrált kockázatkezelési szabályzatban meghatározott Kockázatkezelés módszertana és folyamata alapján megállapított prioritások alapján;

b) ha az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül a cselekvési terv alapján elvégzi az intézkedési terv felülvizsgálatát;

c) ha a meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elvégezni az előírt biztonsági szint elérése érdekében.

(6) Az NKOH az éves költségtervezés során tervezi az informatikai biztonsági stratégia megvalósításához szükséges forrásokat, dokumentálja az előre nem tervezett, de szükséges beruházásokat és biztosítja az intézkedési terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állását.

9. §

Az elektronikus információs rendszerek nyilvántartása

(1) Az IBF az NKOH elektronikus információs rendszereiről folyamatosan aktualizált nyilvántartást vezet. A nyilvántartás minden rendszerre nézve tartalmazza:

a) annak alapfeladatait;

b) a rendszerek által biztosítandó szolgáltatásokat;

c) az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett szervezet kezelésében vannak);

d) a rendszer felett adminisztrációs felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

e) a rendszer felett döntési jogkörrel rendelkező személy személyazonosító és elérhetőségi adatait;

f) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

10. §

Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

(1) A vizsgált rendszerrel kapcsolatos felhasználói, külső és belső hozzáférési engedélyezés a Logikai Védelmi Intézkedések eljárásrendje elnöki utasításban meghatározottak szerint, az ott megadott mellékletek használatával történik. A hozzáféréseket minden esetben az NKOH elnöke engedélyezi.

(2) Az NKOH-nál az információbiztonsággal összefüggő felelősségi köröket a 29. § határozza meg.

(3) Az engedélyezési eljárás során tekintettel kell lenni a felmerülő kockázatokra. Amennyiben a fenyegetettségekkel kapcsolatos változások állnak be, felül kell vizsgálni az integrált kockázatelemzést és jelen IBSZ-t.

11. §

Kapcsolattartás

(1) Az NKOH az érintett szervezetekkel és a hatóságokkal a 247/2014. Korm. rendeletre figyelemmel a rendelkezésre álló feltételrendszer alapján kapcsolatrendszert alakít ki és tart fenn. A hatóságokkal való kapcsolattartásért az egyes szervezeti egységek vezetői felelősek.

(2) Az NKOH a különböző információs csatornákon érkező, az informatikai biztonságot érintő jelzéseket, visszajelzéseket beépíti döntéseibe és érvényesíti tevékenységében, az eredményes működés és a mindkét fél számára előnyös, hosszú távú partnerkapcsolatok kiépítése és fenntartása érdekében.

III. KOCKÁZATKEZELÉS

12. §

Kockázatelemzési eljárásrend

(1) Az NKOH integrált kockázatelemzési stratégiáját az Integrált kockázatkezelési szabályzatban fogalmazza meg, és az érvényes követelmények szerint dokumentálja, valamint közzéteszi. Az Integrált kockázatkezelési szabályzat meghatározza az integrált kockázatelemzési eljárásrend felülvizsgálatának és frissítésének gyakoriságát.

(2) Az NKOH az Integrált kockázatkezelési szabályzatban meghatározottak szerint felülvizsgálja az integrált kockázatelemzések eredményét, megismerteti azt az érintettekkel, amikor változás áll be az elektronikus információs rendszerben vagy

annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre. Az NKOH gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

13. §

Biztonsági osztályba sorolás

(1) Az NKOH minden informatikai rendszerét az adatok bizalmassága, hitelessége, sértetlensége, illetve elvesztésével arányos kárérték szintektől függően az Ibtv., valamint a 41/2015. BM rendelet rendelkezéseinek megfelelően besorolja.

(2) Az NKOH információs rendszerei biztonsági osztályba sorolását a jelen IBSZ *1. számú függeléke* tartalmazza. A biztonsági osztályba sorolást az IBSZ jóváhagyásával az NKOH elnöke hagyja jóvá.

(3) A biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten, de legalább évente el kell végezni, továbbá az intézkedési tervet a biztonsági osztályba sorolásnak megfelelően aktualizálni kell.

(4) Az informatikai rendszerek biztonsági osztályba történő besorolásának megkönnyítése érdekében az NKOH figyelembe veszi az informatikai rendszerek által kezelt adatok körét és érzékenységét.

(5) Vegyes minősítésű (együtt kezelt) adatoknál a legérzékenyebb adat határozza meg a védelem szintjét.

(6) A dokumentumok és adatok kezelése, címkézése az egyes tevékenységi körökkel összhangban történik úgy, hogy azonosításuk és nyomon követésük megfeleljen a feljegyzések kezelésével kapcsolatban az Iratkezelési szabályzatban rögzített irányelvnek.

IV. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS, FEJLESZTÉS ÉS FENNTARTÁS

14. §

Az információbiztonsági erőforrások igényfelmérése

(1) Az NKOH az elektronikus információs rendszerére vonatkozó biztonsági követelmények teljesítése érdekében a rendszerek teljes életciklusában meghatározza, dokumentálja, valamint biztosítja az elektronikus információs rendszer védelméhez szükséges erőforrásokat a beszerzések és közbeszerzések lefolytatásának rendjéről szóló szabályzat szerint. Ennek érdekében folyamatosan figyelemmel kíséri az elektronikus információs rendszerek biztonsági elemeinek megbízhatóságát és teljesítményét. A rendszerek biztonságát érintő igények felmerülése esetén az NKOH kezdeményezi a szükséges eszközök vagy szolgáltatások beszerzését. A beszerzéshez szükséges pénzügyi fedezet rendelkezésre állását a munkamegosztási megállapodással

összhangban a Miniszterelnöki Kabinetiroda Pénzügyi Főosztálya (a továbbiakban: MK PF) vizsgálja.

(2) Az elektronikus információs rendszer beszerzésének engedélyezési folyamata során az alábbiak vizsgálandóak az IBF koordinálásával:

a) a kapacitásigények helytállósága,

b) a tervben megfogalmazottak kielégítik-e az igényeket, elvárásokat,

c) a meglévő rendszerelemekkel való kompatibilitás,

d) a megvalósítás racionalitása.

(3) A megvalósítandó elektronikus információs rendszer-fejlesztéseket szükség esetén információvédelmi szempontból az IBF véleményezi, meghatározva az elvégzendő feladatokat (pl.: kockázatelemzés).

15. §

Információbiztonsági szerződéses követelmények meghatározása

(1) Az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben követelményként az IBF javaslatára az NKOH meghatározza a

a) funkcionális biztonsági követelményeket;

b) a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);

c) a biztonsággal kapcsolatos dokumentációs követelményeket;

d) a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;

e) az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

(2) A megvalósuló fejlesztéseknél a minőségi és biztonsági alapelveket kell követni, lényeges azonban a felhasználói igények precíz megfogalmazása, amit a megrendelésnek vagy szerződésnek kell tartalmaznia.

(3) A szerződés többek között tartalmazza az előző pontban felsorolt feladatok végrehajtására, dokumentumok elkészítésére és átadására vonatkozó előírásokat, a részletes határidőket, költségbecslést és a megállapodás alapjául szolgáló dokumentum hivatkozásokat, mellékleteket, a titoktartási megállapodást és a rendelkezésre állást.

16. §

A rendszer, szoftver átvétele, az elektronikus információs rendszerre vonatkozó dokumentáció

(1) Az új informatikai rendszerekre és a meglévő rendszerek bővítésére vonatkozó elfogadási és átvételi kritériumok a következők:

a) A rendszer leírását, paramétereit, ki- és bemenő adatait, minden olyan további igényt, melyet támaszt az új rendszerrel kapcsolatban, specifikációba kell foglalni és azt mind az NKOH, mind a vállalkozó oldalán el kell fogadni a fejlesztés megkezdése előtt.

b) A specifikáció szerint kell lefolytatni a tesztelést az érintett felhasználók bevonásával.

c) A rendszer, szoftver csak a pozitív eredménnyel záruló tesztelést követően vehető át. A szoftvernek maradéktalanul meg kell felelnie a specifikációnak, továbbá illeszkednie kell az NKOH elektronikus információs rendszeréhez, mind funkcionális, mind biztonsági szempontból.

d) Az NKOH a szerződésben határozza meg az elvárt dokumentációkat, amelyek lehetnek: rendszerterv, rendszerbiztonsági terv, felhasználói kézikönyv, üzemeltetési kézikönyv, üzletmenet-folytonossági terv (BCP), adminisztrátori dokumentáció.

(2) Az adminisztrátori dokumentáció tartalmazza:

a) a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,

b) a biztonsági funkciók hatékony alkalmazását és fenntartását,

c) a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

(3) A felhasználói dokumentáció tartalmazza:

a) a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,

b) a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,

c) a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

(4) Szerződéses követelményként meg kell határozni, hogy a vállalkozó hozza létre és bocsássa rendelkezésre az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a rendszerbiztonsági tervet, továbbá megrendelő erre irányuló igénye esetén a forráskódot, fejlesztési kézikönyvet, valamint a teszt-és futtatókörnyezetet, valamint az üzemeltetés támogatás biztosítását.

(5) A szerződésben kötelezni kell a vállalkozót arra, hogy a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

17. §

Külső elektronikus információs rendszerek szolgáltatásai

(1) Az NKOH figyelemmel kíséri és értékeli a szolgáltatások szerződés szerinti teljesítését és szükség esetén beavatkozik, észrevételeit jelzi a vállalkozók felé.

(2) A szerződéskötés előtt a beszerzéssel érintett szervezeti egység kijelölt munkatársa tisztázza, és amennyiben szükséges rögzíti:

a) a szolgáltatás minőségi, informatikai biztonsági és egyéb követelményeit,

b) a jogszabályi követelmények betartásának szükségességét,

c) az információk sértetlenségének és biztonságának megőrzését,

d) a hozzáférési jogosultságok szükségességét, mértékét, mely megfelel az informatikai biztonsági követelményeknek, és a munka elvégzését lehetővé teszi,

e) az ellenőrzés lehetőségét, körülményeit.

(3) A szolgáltatások szerződés szerinti végrehajtásának, dokumentálásának ellenőrzése és figyelemmel kísérése beszerzéssel érintett szervezeti egység kijelölt munkatársának feladata.

(4) A harmadik fél által nyújtott szolgáltatás feltételeinek változásakor az NKOH mérlegeli annak informatikai biztonsági vonatkozásait, kockázatértékelésre gyakorolt hatását, és amennyiben szükséges, azt a folyamataiban, szabályozási rendszerében átvezeti.

(5) Külső és belső ellenőrzési eszközökkel ellenőrizni kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

18. §

Folyamatos ellenőrzés

(1) A Bkr. rendelkezései alapján az államháztartás egyensúlyának és a közpénzekkel való áttekinthető, hatékony, ellenőrizhető gazdálkodás garanciáinak megteremtése céljából az NKOH belső kontrollrendszert működtet. Ennek keretében az NKOH meghatározza:

a) az ellenőrzendő területeket;

b) az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;

c) az NKOH ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;

d) a mérőszámok megfelelőségét;

e) az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;

f) az NKOH reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére (lásd Incidenskezelés).

(2) Az ellenőrzés megállapításaira, illetve az ellenőrzés értékelésére alapozva intézkedési tervet kell kidolgozni és végrehajtani abban az esetben, ha az ellenőrzés nem tolerálható kockázatot tár fel. Az ellenőrzések eredményét évente értékelni kell.

V. AZ ÜZLETMENET FOLYTONOSSÁG TERVEZÉSE

19. §

Üzletmenet-folytonosságra vonatkozó eljárásrend

(1) Az NKOH egészének működését kialakító, fenntartó és az informatikai biztonságot meghatározó folyamatok, részfolyamatok kerültek kialakításra a szervezetben, melynek szabályozását jelen IBSZ, és az Adminisztratív védelmi intézkedések elnöki utasításban meghatározott Üzletmenet-folytonossági eljárásrend tartalmazza.

(2) Az Üzletmenet-folytonossági eljárásrend kiterjed:

a) a felelősségre,

b) az eljárásrendre,

c) a folyamatokra, részfolyamatokra és kapcsolódási pontokra,

d) eszközökre,

e) a nyomon követhetőségre,

f) a berendezésekre és karbantartásukra,

g) a folyamatváltozásra,

h) az előírt folyamatközi- és végellenőrzésekre, azok dokumentáltságára,

i) a nem megfelelő termékek, a biztonsági incidensek és a gyengeségek kezelésére.

(3) Az Üzletmenet-folytonossági eljárásrend és az Üzletmenet-folytonossági tervek készítése az IBF feladata, az eljárásrend és a tervek készítésekor az események elemzése megtörténik.

20. §

Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

(1) Az NKOH Üzletmenet-folytonossági terveket dolgoz ki a folyamatos működés érdekében. Az Üzletmenet-folytonossági terv lehetővé teszi az NKOH számára a gyors reagálást a feladatának ellátása során bekövetkező zavar, katasztrófa esetére, továbbá rendelkezik az azonnali javításról és forrás biztosításáról a helyreállításhoz.

(2) Az NKOH informatikai rendszerének helyreállítási tervét az Informatikai rendszer helyreállítási terve (a továbbiakban: DRP) tartalmazza. A DRP azokat a tevékenységeket tartalmazza, amelyek a felállított vagy helyreállított informatikai rendszer működőképességét ellenőrzik és biztosítják. A tesztelés minden lépését az üzemeltető jegyzőkönyvben dokumentálja és értékeli. A tesztelést az IBF döntése szerinti gyakorisággal, de legalább évente egyszer kell végrehajtani.

21. §

Üzletmenet-folytonossági tervek felülvizsgálata és értékelése

(1) Az NKOH Üzletmenet-folytonossági tervét annak megfelelősége, hatékonysága érdekében az IBF és az üzemeltető évente felülvizsgálja, továbbá szükség esetén eseti felülvizsgálat keretén belül ellenőrzi, amennyiben

a) az NKOH normál, és/vagy rendkívüli helyzetben történő működését befolyásoló külső, vagy belső dokumentumokban rögzített feltételek, követelmények változtatásra kerülnek,

b) az NKOH működési feltételei, körülményei (fizikai, gazdasági, jogi, stb.) megváltoznak,

c) az informatikai rendszer (szoftver és hardver állomány) fejlesztése történt,

d) az alaptevékenység megváltozik,

e) az NKOH személyi állománya vagy szervezeti felépítése jelentősen megváltozik.

(2) Az (1) bekezdésben rögzített felülvizsgálati tevékenység elvégzése és megállapításainak dokumentálása az IBF feladata és felelőssége.

22. §

Az elektronikus információs rendszer mentései

(1) Az NKOH-nál az információk védelme és az üzletmenet folytonosságának biztosítása érdekében az információkról, szoftverekről és rendszer image-kről az üzemeltető biztonsági másolatot készít és dokumentál, melyek ellenőrzéséért felelős az IBF.

(2) A mentési eljárás célja, hogy biztosítsa a működő rendszerek helyreállíthatóságát. Kidolgozása folyamán magas prioritású szempont, hogy napi mentés készüljön.

(3) A mentések használatáról évente az üzemeltető visszaállítási eljárások alapján meggyőződik. A visszaállításokról jegyzőkönyvet kell készíteni.

23. §

Az elektronikus információs rendszer helyreállítása és újraindítása

(1) Az Üzletmenet-folytonossági terv pontosan kidolgozott utasításokat tartalmaz arra az esetre, ha az elektronikus információs rendszert érintő katasztrófa esetén milyen lépések után állítható helyre a normális vagy a csökkentett kapacitású működés.

(2) Az (1) bekezdés szerinti tevékenységeket az IBF folyamatosan ellenőrzi.

(3) A katasztrófa kezelésére és a helyreállításra vonatkozó előírásokat minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra, így különösen, ha új elektronikus információs rendszer kerül bevezetésre.

(4) Az informatikai rendszer helyreállítási tervét az üzemeltető készíti el. A helyreállítási tervnek olyan technikai részletezettséggel kell elkészülnie, hogy egy megfelelő informatikai rendszerüzemeltetési ismeretekkel rendelkező szakember a szükséges jogosultságok birtokában a rendszer helyreállítását maradéktalanul el tudja végezni.

(5) A működő elektronikus információs rendszerek vészleállításának és újraindításának folyamatát a helyreállítási terv tartalmazza, ezt az üzemeltető állítja össze, és az IBF hagyja jóvá. Az NKOH a dokumentum egy példányát pendrive-on titkosítva tárolja páncélszekrényben.

VI. BIZTONSÁGI ESEMÉNYEK, INCIDENSEK KEZELÉSE

24. §

Biztonsági események, incidensek figyelése

(1) A biztonsági események, incidensek felderítése érdekében az NKOH az elektronikus információs rendszerében az üzemeltető közreműködésével a munkatársak tevékenységeit naplózza.

(2) A naplók kiértékelését és a naplóinformációk alapján történő riasztást automatizált módon kell megoldani.

(3) Az informatikai biztonsági incidensek felderítéséhez, kivizsgálásához az NKOH elnöke és az IBF további naplózást és monitorozást is elrendelhet.

25. §

Hibabejelentés, kezelés

(1) A hiba bejelentése elektronikus levelező rendszeren történik az üzemeltető felé, kivéve, ha a hiba az elektronikus levelező rendszert is érinti, vagy a hiba fontossága miatt nem tűr halasztást. Ebben az esetben szóban vagy telefonon keresztül is lehetséges. A hiba elhárítását a napi működés elsőbbségének megőrzése mellett kell megkezdeni. Amennyiben hiba keletkezik egy informatikai eszközben, akkor azt azonnal jelezni kell az üzemeltető felé, aki intézkedik a szervizeléséről.

26. §

A biztonsági események, incidensek jelentése, kezelése

(1) Az NKOH feladatellátása során felmerülő biztonsági események, incidensek különösen az alábbiak lehetnek:

a) ellenőrzések során feltárt nem megfelelőségek,

b) vonatkozó jogszabályok, előírások megsértése,

c) adatkezelésből, adatfeldolgozásból eredő hiba,

d) kommunikációs hiba, információ torzulás,

e) szoftver zavarok,

f) információvédelem kívülről jövő vagy belülről kiinduló megsértése,

g) ellenőrzések, vonatkozó előírások be nem tartása,

h) emberi hiba, vagy visszaélés,

i) információvédelmi intézkedések be nem tartása,

j) fizikai-környezeti védelem elégtelen volta, meghibásodása,

k) fejlesztések információvédelmi szabályainak be nem tartása,

l) az információvédelmi rendszer működési hibája,

(2) A biztonsági eseményt, incidenst feltáró folyamat egyúttal meghatározza a biztonsági esemény, incidens kezelési tevékenység megvalósításának lehetséges módját, szintjét is.

(3) Az NKOH által nem kezelhető biztonsági eseményeket, incidenseket az üzemeltető biztonsági eseményekké nyilvánítja. Az üzemeltető a biztonsági események, incidensek kezelését az alábbi szabályok szerint végzi:

a) meghatározza, hogy a biztonsági esemény, incidens:

a. okoz-e informatikai rendszer kiesést, vagy meghibásodást,

b. által sérül-e az adatok sértetlensége, hitelessége és bizalmassága (tehát biztonsági esemény kategóriába tartozik-e),

b) kategorizálja (normál, kiemelt, kritikus) és priorizálja a biztonsági eseményt, incidenst,

c) meghatározza a biztonsági esemény, incidens megoldásának végső határidejét.

(4) Az NKOH az üzemeltető közreműködésével a következő tevékenységeket végzi el:

d) az incidens megoldása,

e) hatáselemzés,

f) a megoldás részletes értékelése, dokumentálása,

g) a hibás elem változtatása és amennyiben szükséges a változás tesztelése.

(5) Az üzemeltető a biztonsági esemény, incidens kezelési tevékenység bármely szakaszában dönthet külső szakértő, fejlesztő bevonásáról az NKOH értesítése mellett.

(6) A biztonsági eseményről, incidensről észlelő munkatárs haladéktalanul értesíti jelen IBSZ szerint az üzemeltetőt és az IBF-t, aki intézkedik a hiba kivizsgálása és dokumentálása érdekében az IBSZ *3. számú függeléke* szerint feljegyzés használatával. A munkatársak kötelesek az észlelt vagy gyanított bárminemű biztonsági gyengeséget vagy fenyegetést jelenteni.

(7) A biztonsági esemény, incidens kezelési tevékenység tartalmazza:

a) a nem megfelelőség, biztonsági zavar, működési hiba átvizsgálását,

b) az előidéző okok feltárását,

c) a hibajavítás módját, határidejét,

d) felelősök meghatározását,

e) a hibajavítás eredményének visszaellenőrzését.

(8) A biztonsági esemény, incidens kezelési folyamat lefolytatásáért, a felelős kijelöléséért és a szükséges intézkedések meghatározásáért az IBF felelős. Felelős továbbá az NKOH elnökének tájékoztatásáért, szükség esetén a döntésekbe való bevonásáért.

(9) Az NKOH az üzemeltető közreműködésével a feltárt biztonsági esemény, incidens kezelését elvégzi, melynek során intézkedik a biztonsági esemény, incidens újbóli előfordulásának megakadályozása iránt.

(10) Az NKOH munkatársainak tanácsadást és támogatást nyújt a biztonsági események, incidensek kezeléséhez és jelentéséhez.

VII. EMBERI ERŐFORRÁSOK BIZTONSÁGA

27. §

Álláshelyek, feladatok biztonsági szempontú besorolása

(1) Az NKOH minden álláshelyet, vagy feladatot biztonsági szempontból besorol, továbbá évente felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását. Az NKOH-nál nemzetbiztonsági ellenőrzés alá eső munkakörök vannak.

(2) Az NKOH-nál az informatikai biztonsági szempontból kritikus álláshelyek a következők:

a) elnök

b) üzemeltető

c) IBF

(3) Felelőségi körüket az ügyrendek és a megbízási/vállalkozói szerződés tartalmazza.

28. §

Foglalkoztatottak ellenőrzése

(1) A foglalkoztatási jogviszony létesítésének általános folyamatát az NKOH Közszolgálati Szabályzata, a Kit., a munka törvénykönyvéről szóló 2012. évi I. törvény és egyéb vonatkozó jogszabályi előírások tartalmazzák.

(2) Az NKOH tevékenységéhez szükséges munkakörök betöltésére általános és szakmai feltételeknek való megfelelés esetén nyílik lehetősége a pályázónak.

(3) Az alapkövetelményként teljesítendő általános biztonsági feltételeket az ügyrendek, a munkatársak kinevezési okirata, illetve munkaszerződése tartalmazza.

(4) A felvételkor szükséges igazoló ellenőrzést a Miniszterelnöki Kabinetiroda Személyügyi Főosztálya (MK SZF) és Biztonsági Főosztálya (a továbbiakban: MK BF) végzi, a munkamegosztási megállapodásban foglaltaknak megfelelően

(5) Az informatikai eszközök kiadása az Átadás-átvételi nyilatkozaton kerül kiadásra a munkatárs részére.

(6) Az NKOH munkatársait feladataik maradéktalan és minél magasabb színvonalú ellátása érdekében folyamatosan képezi.

(7) A feladatokat és felelősségeket munkatársak esetében az ügyrendek, a munkatársak kinevezési okirata, munkaszerződés, szerződéses partnerek esetében a vonatkozó szerződés tartalmazza.

29. §

Eljárás a jogviszony megszűnésekor és megváltozásakor

(1) A foglalkoztatási jogviszony megszűnéséhez vagy megváltozásához kapcsolódó feladatok teljesítése szorosan kapcsolódik az információ kezelés és informatikai biztonság tárgyköréhez. A foglalkoztatási jogviszony létrejöttét megelőző időszaktól a munkaviszony megszűnését követő időszakig terjednek, folyamatosan biztosítva az NKOH érdekei sérülésének elkerülését, vagy lehetőségének minimálisra csökkentését.

(2) A foglalkoztatási jogviszony megszűnéséhez vagy megváltoztatásához közvetlenül kapcsolódó adminisztrációs feladatok elvégzése az NKOH Koordinációs és Titkársági Osztály, valamint az MK SZF és MK BF feladata. A munkakörhöz kapcsolódó számítástechnikai eszköz, kulcs, stb. visszavétele dokumentáltan megtörténik.

(3) Az üzemeltető az NKOH Koordinációs és Titkársági Osztály írásbeli tájékoztatása alapján megszünteti vagy megváltoztatja a munkakörhöz tartozó hozzáférési jogosultságokat. A névre szóló postafiókra érkező levelek esetén az automatikus válaszadás beállíttatása is az üzemeltető feladata.

30. §

A munkatársakkal szemben támasztott elvárások megfogalmazása

(1) A hozzáférési jogosultságot igénylő munkatárssal szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket jelen IBSZ, valamint az adott rendszer felhasználói dokumentációjának kell tartalmaznia.

31. §

A rendszer használattal kapcsolatos információk biztosítása

(1) A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő munkatársnak írásbeli nyilatkozatott kell tennie arról, hogy az érintett rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

32. §

A felhasználókkal szemben támasztott elvárások felülvizsgálata

(1) Évente az IBF-nek és az üzemeltetőnek felül kell vizsgálni a rendszerek használatával kapcsolatban a munkatársakkal szemben támasztott elvárásokat. Abban az esetben, ha a rendszeres felülvizsgálat során vagy azon kívül megállapítást nyer, hogy a rendszer szolgáltatásai, funkcionalitása, hatóköre megváltozott vagy más okból következően az

elvárásokban változás állt be, az üzemeltetőnek haladéktalanul jelentenie kell ezt az IBF felé és tájékoztatnia kell a rendszer felhasználóit.

(2) A tájékoztatás történhet e-mail-ben vagy nagyobb változás esetén erre a célra megszervezett oktatáson. E-mail tájékoztatás esetén az egyes felhasználóknak e-mail-ben vissza kell jelezniük, hogy az e-mail-ben kapott tájékoztatást megértették és a jövőben annak alapján járnak el.

33. §

A szerződéses partnerekre vonatkozó követelmények

(1) Az NKOH azonosítja az információit és információ-feldolgozó eszközeit fenyegető kockázatokat, melyek olyan működési folyamatokból származnak, amelyekben külső felek vesznek részt, ezekkel szemben megfelelő, dokumentált és jóváhagyott intézkedéseket hoz és érvényesít a hozzáférési jog megadása előtt.

(2) Az informatikai rendszerrel kapcsolatba kerülő, vagy az informatikai biztonságra hatást gyakorló külső személyekkel olyan írásbeli megállapodást – titoktartási megállapodás – kell kötni, amely vagy tartalmazza, vagy utal minden olyan informatikai biztonsági követelményre, amely megteremti az IBSZ-nek és a bevezetett szabályoknak való megfelelést.

(3) Az NKOH elektronikus információs rendszeréhez és információihoz külső fél számára megfelelő hozzáférést adni az IBSZ és a hozzá kapcsolódó folyamatleírások megismerése, valamint a titoktartási megállapodás aláírása után lehet.

(4) Külső személyekkel megkötött szerződés tartalmi előírásait a beszerzési szabályzat tartalmazza.

34. §

Személyi biztonsággal kapcsolatos logikai védelmi intézkedések

(1) Amennyiben a személyi biztonsággal kapcsolatos követelmények változnak, azokat az érintettekkel közölni kellés a megismeréséről újbóli nyilatkozattétel szükséges.

(2) A személyi biztonsággal kapcsolatos követelmények egyaránt vonatkoznak a rendszerhez hozzáférési jogosultsággal rendelkező munkatársakra és az NKOH szerződéses partnereire.

(3) Az (2) bekezdés szerinti személyi biztonsággal kapcsolatos követelmények teljesítése körében a munkatársak, valamint a szerződéses partnerek kötelesek:

a) a rendszert és annak adatait az előírásoknak, kézikönyveknek, útmutatóknak megfelelően, rendeltetésszerűen használni, annak hibáit, biztonsági hiányosságait észleléskor jelenteni;

b) a hitelesítő eszközeiket saját ellenőrzés alatt tartani és biztonságos őrzéséről gondoskodni, ezek kompromittálódását haladéktalanul jelenteni;

c) a jelen IBSZ-ben megfogalmazott internetes viselkedési szabályokat betartani, az NKOH-t felelősen, a vonatkozó felhatalmazásnak megfelelően képviselni;

d) az NKOH adatait maximális körültekintéssel kezelni, azok bizalmasságát és integritását megőrizni;

e) a hozzáférésnek megfelelően az IBSZ vonatkozó részeit megismerni és betartani.

35. §

Fegyelmi intézkedések

(1) Az emberi tényezőkből eredő informatikai biztonsági események és zavarok bekövetkezése esetén az NKOH elnöke a vonatkozó munkajogi és az informatikai biztonsághoz kapcsolódó más előírások betartása mellett egyedi elbírálás alapján jár el.

(2) Szándékos emberi hiba, mulasztás, vagy az NKOH-t érő erkölcsi és pénzügyi veszteség, hatás esetén az IBF javaslata alapján az NKOH elnöke jár el a Közszolgálati szabályzat által szabályozott fegyelmi eljárás keretében.

36. §

Viselkedési szabályok az interneten

(1) A munkatársak csak az ügyrendben és a kinevezési okiratukban rögzített feladatok ellátása érdekében használhatják az internetet. Az internethez való csatlakozás módja csak ellenőrzött módon, központilag történhet tűzfallal védett vonalon.

(2) Különösen tilos a fájlcserélők és tartalom megosztók működtetése, illetve egyéni szórakozást biztosító programok, filmek, audió fájlok letöltése, a csevegő szobákba belépés.

(3) Tilos a felhasználóknak a munkaállomásra telepített böngészők biztonsági beállításait megváltoztatni.

(4) Az internet használata és az általa megvalósított bármely cselekmény kizárólag a törvények és egyéb szabályok keretei között megengedett.

(5) Az üzemeltető az NKOH elnökének megbízásából a forgalmi adatokat esetenként ellenőrzi. Ha a statisztikák alapján megállapítható, hogy a felhasználó jogosultságait munkakörétől eltérő célra használja, az elnöknek azonnali hatállyal a jogosult a jog visszavonására.

(6) Az internet használata során a munkaállomásokon történő bizalmas adatkezelés mellett nyilvános, nem ellenőrzött adatforrásokból is fogadhat adatokat a felhasználó. Tekintettel erre, az alábbi intézkedések betartása kötelező:

a) Tilos szoftverek letöltése során a szoftver tulajdonosa által szabott jogi feltételeket megszegni.

b) Az internetről letöltött fájlokat csak vírusellenőrzés után szabad megnyitni.

c) A hálózati védelmet biztosító eszközt kikerülni tilos.

d) Tilos a munkahelyi e-mail cím használata, megadása szórakoztató tartalmú oldalon.

(7) A munkatársak az ügyrendben és a kinevezési okiratukban rögzített feladatok ellátása során csak a NKOH által biztosított e-mail címeket használhatják. A munkatársak internet postacíme a következőképpen alakul: keresztnév.vezetéknév@nkoh.gov.hu.

(8) Az NKOH elektronikus levelezés céljára exchange levelezőszerver programot alkalmaz.

(9) A levelezőrendszer felhasználói jogosultságaival kapcsolatos teendők ellátása az általános felhasználó jogosultságkezelés keretein belül megtörténik.

(10) A leveleket víruskereső és spam szűrő alkalmazások szűrik a levelező szerveren, mindkettő adatbázisa automatikusan frissül. Minden felhasználó felel a hozzá rendelt felhasználói azonosítóval elkövetett visszaélésekért.

(11) Tilos a felhasználóknak olyan tartalmú elektronikus levelet az NKOH informatikai rendszeréből küldeni, amely az NKOH érdekeivel ellentétes.

(12) Az NKOH-ból személyes adat nem továbbítható harmadik személy számára elektronikus levélben.

(13) Az NKOH-ból külső szerverre adatok, információk kiküldésénél az informatikai biztonsági szempontokat a küldőnek minden esetben figyelembe kell venni.

(14) Az üzemeltető az egyes fájltípusok, illetve az ún.: „levélszemét" forgalmát a levelező szerver beállításaival letilthatja, vagy blokkolhatja. Amennyiben a munkavégzés okán ilyen jellegű fájl forgalmára van szükség, a tiltás feloldását írásban kell kérni.

(15) Mivel mind az e-mail, mind az internet forgalom az NKOH által biztosított eszközökön történik, és ezen eszközök biztosítása a munkafolyamatok ellátásával kapcsolatos tevékenység megkönnyítésére irányul. Az NKOH elnöke jogosult az NKOH e-mail címein bonyolított levelezést, illetve az interneten látogatott oldalakat, temporális internet fájlokat, letöltéseket a felhasználó gépén, vagy a szerveren ellenőrizni.

(16) Az internethez való csatlakozás módja csak ellenőrzött módon, központilag történhet a tűzfallal védett vonalon. Internetre modemes vagy mobil kapcsolaton keresztül feljelentkezni miközben a helyi hálózatba is kapcsolódva van a munkaállomás tilos. A mobil internet használata csak külön engedély alapján történhet.

VIII. TUDATOSSÁG ÉS KÉPZÉS

37. §

Biztonság tudatosság képzés

(1) A biztonság tudatossági képzés célja, hogy a munkatársak képesek legyenek biztonságosan használni az informatikai rendszert, legyenek tudtában a rendszerre ható fenyegetettségeknek, ezáltal az NKOH minimalizálni tudja a munkatársakra ható veszélyforrások bekövetkezéséből fakadó károk hatásait.

(2) A biztonság tudatossági képzés célja továbbá, hogy a munkatársak megismerjék a rájuk vonatkozó szabályokat, legyenek tisztában a jogaikkal és kötelességeikkel. A belépő új felhasználók még az IT rendszerhez történő hozzáférés előtt ismerjék meg a biztonsági előírásokat.

(3) A biztonság tudatossági képzéssel gondoskodni kell arról, hogy a napi feladatok végzése során a munkatársak kellőképpen felkészültek legyenek:

a. a védelmi intézkedésekre vonatkozó szabályzások betartására;

b. a lehetséges belső fenyegetések felismerésére;

c. az alapvető biztonsági követelmények betartására.

(4) A biztonsági előírásokat új munkatársak kezdeti képzésének részeként, egyébként évente, vagy amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi, oktatni kell.

(5) Az IBF kötelessége az oktatási anyag szakmai részének elkészítése, naprakészségének és minden felhasználó részére való hozzáférhetőségének biztosítása, valamint az oktatások megtartása, melyben

a. fel kell hívnia a munkatársak figyelmét az informatikai biztonsági rendszerben bekövetkezett változásokra és azok indokaira,

b. ismertetnie kell azokat a sebezhetőségeket, melyek a munkatárs adat és rendszer biztonságát veszélyeztető magatartását használják ki.

(6) Az IBF kötelessége az oktatási anyag és oktatási tematika szerint felhasználói biztonság tudatosság építő oktatást megtervezni és megszervezni, amennyiben szükséges külső tanácsadó bevonásával.

(7) Minden új felhasználót kötelező a felhasználói jogosultság biztosítását megelőzően biztonsági oktatásban részesíteni.

(8) A biztonsági oktatások megtörténtét jelenléti íven kell dokumentálni, melyen a képzésen résztvevők a képzés megtörténtét, az elhangzottak megismerését és megértését elismerik, és ezt a dokumentumot megőrzi.

IX. FIZIKAI VÉDELMI INTÉZKEDÉSEK

38. §

A biztonsági területek

(1) Az NKOH a nem engedélyezett, illetéktelen hozzáférést és behatolást továbbá az ebből következő károkat a Fizikai védelmi intézkedések eljárásrend elnöki utasításban dokumentált fizikai és környezeti védelem intézkedések kihirdetésével és megvalósításával előzi meg.

X. LOGIKAI VÉDELMI INTÉZKEDÉSEK

ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

39. §

Engedélyezési folyamatok

(1) Az adatfeldolgozás csak akkor engedélyezhető, ha az az adatkörök biztonsági osztályba sorolásának megfelelő adatfeldolgozó eszközökön történik – ideértve az összeférhetetlenséggel kapcsolatos szabályozások megtartását is.

(2) Az NKOH elnöke az új adatfeldolgozási eszközökre és adatfeldolgozási lehetőségekre vonatkozó jóváhagyását csak abban az esetben adja meg, ha azok megfelelnek a kiszolgált alkalmazások védelmi osztályának, az arra előírt biztonsági feltételeknek.

(3) Az üzemeltetőnek ellenőrzéssel kell meggyőződni a hardver, szoftver eszközök és más rendszer összetevők kompatibilitásáról.

(4) Az adatokat feldolgozó új rendszer használata az IBF tájékoztatásával és szükség szerinti véleményezésével történhet.

40. §

Az elektronikus információs rendszer kapcsolódásai

(1) Az NKOH csak a felügyelete alatt álló informatikai rendszer felett gyakorol kontrollt, a rendszer felügyelet nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett. Az NKOH munkatársai felügyelete alatt álló, ideiglenes kapcsolatok így az adatok manuális letöltése más szervezetek informatikai rendszeréből, nem tartoznak e tiltás hatálya alá.

XI. TERVEZÉS

41. §

Biztonságtervezési eljárásrend

(1) Az NKOH informatikai rendszerek fejlesztése jelen IBSZ-ben meghatározottak szerint történik. Az NKOH új rendszerek fejlesztésekor vagy meglévő rendszerek bővítésekor a biztonsági követelményeket a fejlesztés minden szakaszában vizsgálja és értékeli az érintett elektronikus információs rendszer biztonsági osztályba sorolásának tükrében. A biztonsági osztályba sorolás alapján meghatározott követelménynek megfelelő rendszerfejlesztés, -bővítés engedélyezhető.

42. §

Rendszerbiztonsági terv

(1) Az NKOH a rendszerek fejlesztésekor vagy meglévő rendszerek bővítésekor gondoskodik a vállalkozó illetve üzemeltető által készített olyan rendszerbiztonsági terv rendelkezésre állásáról, amely:

a) összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával;

b) meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait, biztonságkritikus elemeit és alapfunkcióit;

c) meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;

d) meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

e) a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;

f) meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;

(2) Az NKOH gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék.

(3) Az NKOH a vállalkozó illetve üzemeltető közreműködésével legalább évente felülvizsgálja, az elektronikus információs rendszer rendszerbiztonsági tervet, valamint frissíti, amennyiben az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák ezt indokolják. Az NKOH gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

(4) Az NKOH-nál üzemeltetett rendszerek alapfeladatát jelen IBSZ *2. számú függeléke* szerinti információs rendszer-nyilvántartás tartalmazza.

(5) A rendszerbiztonsági tervet az NKOH elnöke, a vállalkozó illetve az üzemeltető és az IBF ismerheti meg. A rendszerbiztonsági tervet az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell súlyos, a rendszerrel összefüggő biztonsági esemény bekövetkezése esetén vagy annak környezetébe az információbiztonságra releváns hatással bíró változás esetén.

(6) A rendszerbiztonsági tervet automatikusan frissíteni kell minden rendszerbiztonsági tervben rögzített információ változása, illetve új, a rendszerrel összefüggő új információ megismerése esetén.

XII. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

43. §

A rendszer fejlesztési életciklusa

(1) Az NKOH az elektronikus információs rendszerének teljes életútján, azok minden életciklusában az IBF által figyelemmel kíséri az informatikai biztonsági helyzetet. A fejlesztések életciklusainak egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint az NKOH-re

vonatkozóan meghatározza az információbiztonsági szerepköröket betöltő személyeket.

(2) Az NKOH a rendszerére vonatkozóan az alábbi életciklus szakaszokat határozza meg:

a) követelmény meghatározás,

b) fejlesztés vagy beszerzés,

c) megvalósítás vagy értékelés,

d) üzemeltetés és fenntartás,

e) kivonás (archiválás, megsemmisítés).

(3) A rendszer fejlesztését végző külső vállalkozóval kötött szerződés kitér az NKOH által elvárt információ biztonsági követelményekre. A külső vállalkozónak a szerződés alapján lehetővé kell tennie az információ biztonsági követelmények ellenőrzését az NKOH számára.

XIII. BIZTONSÁGI ELEMZÉS

44. §

Biztonságelemzési eljárásrend

(1) Az NKOH-nál bevezetett szabályozások és azok betartásának ellenőrzése biztosítja, hogy az NKOH tevékenységéhez kapcsolódó összes biztonsági eljárás megfelelő módon kerüljön végrehajtásra. A Biztonságértékelési eljárásrend szerinti rendszeres felülvizsgálat tárgyát képezi a biztonsági politikának és alkalmazott jogszabályoknak való megfelelés biztosítása.

(2) Az adott tevékenységre vonatkozó szabályozásokat az IBSZ és a Védelmi intézkedések eljárásrendek, az ellenőrzéseket az adott tevékenységet meghatározó dokumentumok (pl.: Belsőellenőrzési szabályzat) rögzítik.

(3) Az információs rendszerek rendszeres ellenőrzésére az IBF éves terve alapján kerül sor a védelmi jogszabályoknak való megfelelés biztosítása céljából.

(4) Az NKOH informatikai biztonsági rendszerének független felülvizsgálatára több megoldást alkalmazhat:

a) belső ellenőrzés

b) IBF

c) szerződéses kereteken belül független külső auditorok

közreműködésével, ezáltal biztosítva, hogy a szervezet gyakorlata megfelelően tükrözze a szabályozást és hatékony módon működtethető legyen.

(5) Az NKOH az IBF koordinálásával fejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét. A biztonsági teljesítmény mérése kiterjed:

a) a feltárt hiányosságok alakulására,

b) biztonsági incidensek alakulására,

c) védelmi rendszeren átjutó behatolási kísérletek alakulására,

d) hálózati vagy rendszer leállások időtartamára,

e) üzletmenet folytonosságot akadályozó incidensek alakulására,

f) üzemeltetési adatokra,

g) kapacitási adatokra,

h) rendelkezésre állásra.

XIV. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

45. §

Sérülékenység teszt

(1) Az NKOH az IBF javaslatára az üzemeltetővel vagy megbízott vállalkozóval az elektronikus információs rendszere tekintetében sérülékenység tesztet végeztet, amennyiben azt az elektronikus információs rendszer fejlesztési, üzemeltetési és használati körülményei lehetővé teszik, lehetőleg évente, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet.

(2) Az NKOH a sérülékenységeket az alábbi elvek mentén kezeli:

a) interneten elérhető határvédelmi eszközeit sérülékenység vizsgálatnak veti alá,

b) belső eszközeit eseti jelleggel vizsgálja meg.

(3) A sérülékenység tesztet végző kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról, végrehajtja az ellenőrzési listákat és tesztelési eljárásokat, felméri a sérülékenység lehetséges hatásait, elemzi a sérülékenység teszt eredményét, ismerteti az eredményt az IBF-el.

(4) Az NKOH olyan sérülékenységi teszteszközt alkalmaztat, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.

(5) Az NKOH az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizáltatja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.

(6) Az NKOH a sérülékenységi teszt végrehajtásához a sérülékenységi vizsgálatot végző személynek a vizsgálat idejére hozzáférést biztosít az NKOH az elektronikus információs rendszeréhez.

(7) A sérülékenységi vizsgálat után az IBF-nek fel kell mérnie, hogy egy támadó milyen érzékeny adatokhoz lehet képes hozzáférni a NKOH információvagyonából. A vizsgálatot követően kockázatelemzés hatására az NKOH intézkedéseket foganatosít az érzékeny adatok megismerésének elhárítására.

XV. KONFIGURÁCIÓKEZELÉS

46. §

Konfigurációkezelési eljárásrend

(1) Az NKOH a Logikai védelmi intézkedések elnöki utasításban meghatározott konfigurációkezelési eljárásrendben dokumentált konfigurációkezelés kihirdetésével és megvalósításával biztosítja a folyamat elvárt működését és ellenőrizhetőségét.

(2) Az NKOH-nál a sértetlenség felülvizsgálatára vonatkozó megállapításokat a vonatkozó független felülvizsgálatok jegyzőkönyvei tartalmazzák.

(3) Az NKOH az informatikai infrastruktúra konfigurációit és azok alkotó elemeket több szintre lebontva tartja nyilván, ily módon lehetővé teszi azok hatékony kezelését. Általánosságban a lebontás addig a szintig történik az egyes konfiguráció elemek esetében, amely egységnél jelentkeznek vagy jelentkezhetnek a változtatások.

(4) Az NKOH informatikai rendszerei kapcsán biztosítja, hogy azok biztonságosan legyenek beállítva, azaz konfigurálva. Ennek érdekében a következő szabályokat érvényesíti:

a) az informatikai rendszereket szállító, illetve üzemeltető szerződött partnerektől megköveteli a biztonságos beállítást elvégzését;

b) az alapkonfiguráció rögzítésre kerül;

c) változás kezelés van bevezetve;

d) érvényesíti a legszűkebb funkcionalitás elvét;

e) az információs rendszerelemekről leltár készül.

47. §

A szoftverhasználat korlátozásai, telepített szoftverek

(1) A szellemi tulajdonjogok védelme érdekében az NKOH a vonatkozó jogszabályi előírásokat betartja és betartatja. A szoftvertermékek felhasználására vonatkozó korlátozást, az illegális szoftverek használatának megakadályozását az NKOH biztosítja. A szellemi tulajdonjogokkal rendelkező szoftverek és a hozzájuk tartozó licencek elektronikus nyilvántartását és őrzését az üzemeltető végzi. A nyilvántartás tartalmazza a szoftver nevét, a felhasználható licencek számát és a felhasználókat. A licencgazdálkodásért az üzemeltető felelős.

(2) A számítógépekre történő szoftvertelepítést csak az üzemeltető végezhet, más szoftver önállóan nem telepíthető.

(3) A szoftverek másolása egyik gépről a másikra, illetve bármilyen más adathordozóra tilos, ha azt nem a munkafolyamatok követelik meg. Ilyen feladatok végrehajtásánál mindig meg kell győződni a szoftverek jogvédelmének érvényre jutásáról.

(4) AZ NKOH által felhasználási vagy tulajdonjoggal rendelkező szoftverek az NKOH vagyonát képezik, eltulajdonításuk sérti az érdekeit. Ezért tilos ezeket az NKOH-ból adathordozón kivinni, a szervezeten kívüli személy vagy külső cég részére átadni, másolni vagy hozzáférhetővé tenni – beleértve a hálózaton vagy Interneten való hozzáférés lehetőségét is –, kivéve, ha erről a hatályos szerződések másként rendelkeznek.

XVI. KARBANTARTÁS

48. §

Karbantartási eljárásrend

(1) Az NKOH a Logikai védelmi intézkedések elnöki utasításban meghatározott karbantartási eljárásrendben dokumentált karbantartások kihirdetésével és megvalósításával biztosítja a folyamat elvárt működését és ellenőrizhetőségét.

(2) Az NKOH-nál az üzemeltető gondoskodik a központi szolgáltató szerver megelőző jellegű karbantartásáról, a folyamatos rendelkezésre állásuk és sértetlenségük érdekében. Egyéb eszközöknél, berendezéseknél eseti javítás történik.

(3) Az NKOH informatika rendszerének megbízható működése érdekében rendszeres karbantartást kell végezni az informatikai üzemeltetés részeként.

(4) A karbantartást tervezetten, előre bejelentve végezhető.

(5) A karbantartást végző személyek, illetve szerződött partnerek esetében a biztonsági szempontokat messzemenően figyelembe kell venni, amelyek a következők:

a) szakértelem igazolása;

b) azonosítás és hitelesítés;

c) gyártói előírások betartása.

XVII. ADATHORDOZÓK VÉDELME

49. §

Adathordozó kezelési és védelmi eljárásrend

(1) Az NKOH a Logikai védelmi intézkedések elnöki utasításban meghatározott adathordozó kezelési és védelmi eljárásrend dokumentált kihirdetésével és megvalósításával biztosítja a folyamat elvárt működését és ellenőrizhetőségét.

(2) Az NKOH az adathordozók jelentette kockázatok csökkentése érdekében a következő intézkedéseket teszi:

a) meghatározza az adathordozókhoz hozzáférők körét,

b) előírja az adathordozók biztonságos törlési eljárását,

c) engedélyezi, illetve korlátozza a mobil adathordozók használatát.

XVIII. AZONOSÍTÁS ÉS HITELESÍTÉS

50. §

Azonosítási, hitelesítési, hozzáférés-felügyeleti eljárásrend

(1) Az NKOH a Logikai védelmi intézkedések elnöki utasításban meghatározott azonosítási, hitelesítési, hozzáférés-felügyeleti eljárásrend dokumentált kihirdetésével és megvalósításával biztosítja a folyamat elvárt működését és ellenőrizhetőségét.

(2) A komplex hozzáférés felügyelet magában foglalja a számítógépes rendszerben tárolt adatállományokhoz, illetve a feldolgozás alatt álló adatokhoz való hozzáférés személyhez kötött naplózását, az iratokba való betekintés naplózását, bizalmas tárgyú értekezleteken, megbeszéléseken résztvevők nyilvántartását, bizalmas szóbeli közléseket illetően a kommunikáló felek személyhez kötött dokumentálását.

(3) Az információvédelmet biztosító informatikai rendszerben az NKOH biztosítja:

a) ahol indokolt, az üzemeltető kialakítja a többszintű hitelesítési és azonosítási rendszert az egyes szoftverek által nyújtott biztonsági funkciók, az alkalmazási területek és a biztonsági követelmények figyelembevételével.

b) A hozzáférés jogosultság menedzselésénél az NKOH a következő hozzáférési jogokat alkalmazza:

i. olvasási jog (betekintés),

ii. írási jog (létrehozás),

iii. módosítás és törlési jog.

c) A rendszer objektumaihoz (fájlok, eszközök, processzek közötti kommunikációs csatornák) egyedi, illetve csoport tulajdonosokat rendel az objektum létesítésekor. A hozzáférés vezérlése esetén az adott objektumhoz (pl. fájl) esetenként (pl. létesítéskor) rendelődnek hozzá a tulajdonosok jogai is.

d) A hozzáférési események esetén a jogosultság ellenőrzés automatikusan történik.

e) A jogosultsági rendszer támogatja a jogosultságok módosítását, törlését és időleges korlátozását. Új jogosultság kiosztását, a jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott végezheti el.

f) A jogosulatlan hozzáférési kísérleteket a biztonsági napló automatikusan rögzíti, ennek értékelését az üzemeltető biztonsági incidens esetén szükség szerint elvégzi.

(4) Az azonosítási, hitelesítési, hozzáférés-felügyeleti eljárás biztosítja:

a) az egyedi felhasználó azonosítást, mellyel a felhasználók tevékenysége követhető,

b) az informatikai rendszerek, adatbázisok használata esetén a hozzáférés jogosultságának ellenőrzését,

c) a hozzáférési jogosultságok meghatározása és kiosztása az NKOH informatikai biztonsági politikájának megfelelő módon történik, a hozzáférési jogosultságok meghatározása az adott terület vezetőjének írásos engedélye alapján az üzemeltető vagy az alkalmazás felelős feladata,

d) hogy a felhasználók ismerik a hozzáférési lehetőségeiket, megértik és alkalmazzák azokat,

e) jogosultság nélküli hozzáférés megakadályozását, kivizsgálását,

f) a hozzáférési jogosultságok azonnali megszüntetését, amikor az szükségessé válik (pl.: munkaviszony megszűnése),

g) a felhasználó hozzáférési jogainak belépéskor illetve új munkakörbe helyezésekor a vezető írásban történő engedélyezése után, a hozzáférési jogosultságok megváltoztatását.

Ezen végrehajtása, dokumentálása az üzemeltető vagy az alkalmazásfelelős, a feladatok elvégzésének ellenőrzése az IBF feladata.

A dokumentált hozzáférési jogosultság meghatározása a szerződéses partnerekkel, alvállalkozókkal kialakított kapcsolat jellegétől, valamint az alvállalkozói tevékenység tárgyától függ, azonban minden esetben meghatározásra kerül a hozzáférés módja és mértéke, valamint az NKOH informatikai biztonságra vonatkozó követelményei.

51. §

A felhasználó felelősségei

(1) Az NKOH-nál minden munkatárs felelős azért, hogy munkahelyén csak a munkahelyi programokat használja, idegen programot, adatot oda ne vigyen (így vírust sem), és munkahelyéről engedély nélkül nem hozhat el sem adatot, sem programot. Jogosulatlanul nem juttathat ki védett információkat, adatokat, akár állományokat az NKOH-ból, csak az informatikai biztonsági alapelveknek megfelelően.

(2) Az NKOH-nál a munkatársak kötelesek betartani a bevett biztonsági gyakorlatot a jelszó kiválasztása, felhasználása és változtatása során. A munkatársaknak első bejelentkezés alkalmával a kötelező jelszócserét végre kell hajtani, illetve megváltoztatják az üzemeletető által meghatározott időszakonként.

(3) Mindenki köteles a rá bízott és az általa beállított jelszavak titkosságát megőrizni. A jelszó ismertté válása esetén a jelszót meg kell változtatni.

(4) Automatikus bejelentkezési eljárások (pl. batch fájlok, vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót.

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

(6) A munkatársak gondoskodnak arról, hogy a használaton kívüli felszerelések megfelelő védelemben részesüljenek a jogosulatlan hozzáféréssel szemben.

(7) A munka megszakításakor minden dokumentumot menteni kell és lehetőség szerint az ablakokat be kell zárni. A munkaidő végén a munkaállomást szükséges kikapcsolni.

52. §

Ellenőrzés

(1) Az IBF ellenőrzi az azonosítással és hitelesítéssel kapcsolatos előírások maradéktalan betartását. Ennek során ellenőrizni kell, hogy:

a) a felhasználói azonosítók és jelszók tartalmi követelményeire vonatkozó előírások érvényesülését;

b) a felhasználói azonosítók és jelszavak/tanúsítványt hordozó eszközök kezelésre vonatkozó előírások érvényesülését;

c) a felhasználói azonosítók és jelszavak/tanúsítványt hordozó eszközök nyilvántartásának naprakészségét.

53. §

Hitelesítés szolgáltatók tanúsítványának elfogadása

(1) Az NKOH elektronikus információs rendszerei csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el az NKOH-n kívüli felhasználók hitelesítéséhez.

XIX. HOZZÁFÉRÉS-ELLENŐRZÉS

54. §

Rendszer és alkalmazás hozzáférés szabályozás

(1) A hozzáférési jogosultságok szabályozásával, és jelszó azonosítási rendszer használatával az NKOH biztosítja, hogy a munkatársak csak azokhoz a szolgáltatásokhoz férhetnek hozzá közvetlenül, amelyek használatára kifejezetten fel vannak hatalmazva.

(2) Az NKOH távoli felhasználók hozzáférése esetén a felhasználókat minden esetben az informatikai rendszerben azonosítja, a biztonságos hozzáférést megoldja. A távoli felhasználói hozzáférést mindig hitelesítéssel végezteti.

(3) A hozzáférés korlátozása a következő módokon történhet:

a. a felhasználók kizárása azoknak a feladatoknak az elvégzéséből, amelyekhez egyébként nem rendelkeznek jogosultságokkal,

b. az információvagyon védelmi besorolásának figyelembe vétele az információ megjelenítésénél és továbbításánál.

55. §

_Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

(1) Az NKOH-ban használt informatikai rendszerben nem engedélyezett azonosítás vagy hitelesítés nélkül végzett tevékenység.

56. §

Hordozható számítógépes eszközök

(1) A hordozható számítógépes eszközök (laptopok, tabletek) esetében a munkatárs felelős a fizikai védelem megvalósításáért. A hordozható számítógépes eszközök használata során kiemelt hangsúlyt fektet az eszközön tárolt adatok védelmére.

(2) A hordozható számítógépek csak az NKOH informatikai biztonsági politikáját kielégítő biztonságú operációs rendszerrel használhatóak.

(3) Az NKOH a hordozható számítógépes eszközök külső felhasználása során különös gondot fordít az eszközök fizikai és adatvédelmére. A fizikai védelemért a hordozható eszköz felhasználója felel, továbbá elvégzi az adatszinkronizálást az NKOH központi rendszere és a hordozható eszköz között.

(4) A hordozható számítógépes eszközök hálózatra történő csatlakozásakor a vírusvédelemnek automatikusan meg kell újulnia, és működésbe kell lépnie.

57. §

Külső elektronikus információs rendszerek használata

(1) Külső rendszerből történő hozzáférés esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről. Távmunka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.

(2) A bejelentkezés időtartamára a felhasználóra érvényesek az általános informatikai biztonsági szabályok.

(3) A rendszerbe való belépéshez szükséges a belépő munkatárs azonosítása (felhasználói azonosító / jelszó megadása). A belépési azonosítókat másra átruházni, illetve más azonosítóját használni nem szabad.

(4) A belépési adatokat titkosságának megőrzéséért a munkatárs felelős.

(5) A bejelentkezéseket ellenőrizni és naplózni kell.

(6) A bejelentkezett végpontot nem szabad felügyelet nélkül hagyni, még rövid időre sem. A gépet minden esetben lockolt állapotban kell hagyni.

(7) 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani.

(8) A számítógépen vírusvédelmi rendszernek kell telepítve lennie, és ezt kötelező használni.

58. §

Nyilvánosan elérhető tartalom

(1) Az NKOH elnöke vagy az általa felhatalmazott munkatárs jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az NKOH-val kapcsolatos bármely információ közzétételére. A felhatalmazott munkatársakat biztonságtudatossági képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat.

(2) A felhatalmazott munkatárs közzététel előtt átvizsgálja a javasolt tartalmat, továbbá félévente rendszeresen átvizsgálják a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat.

(3) Tilos az interneten publikálni az informatikai rendszerre vonatkozó bármilyen információt.

XX. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

59. §

Rendszer- és információsértetlenségre vonatkozó eljárásrend

(1) Az NKOH az információkezelésre szolgáló eszközeinek használatát, az információhoz való hozzáférés szabályait, az információ kezelés, tárolás és feldolgozás szabályait, valamint a kapcsolódó felelősségek meghatározását jelen IBSZ szabályozza.

(2) A Logikai védelmi intézkedések elnöki utasításban meghatározott rendszer- és információsértetlenségre vonatkozó eljárásrend kitér a normál üzletmenetre, továbbá a hibák kezelésére, szokásostól eltérő, váratlan üzemeltetési és műszaki feltételek kezelésére, az ellenőrzési és dokumentálási kötelezettségekre.

(3) Az NKOH biztosítja a rendszer-és információsértetlenség kapcsán:

a. a változások azonosítását, nyomon követését, dokumentálását,

b. a változtatások potenciális hatásának értékelését a kockázatok értékelésére, védelmi intézkedésre,

c. az engedélyezés folyamatát,

d. a változtatásokkal érintett személyek tájékoztatását, amennyiben szükséges, oktatások lebonyolítását.

(4) Az üzemeltető évente felülvizsgálja a rendelkezésre álló erőforrások felhasználását, vizsgálja a fellépő igényeket, jövőbeni kapacitás szükségleteket, ennek megfelelően javaslatot tesz a szükséges fejlesztésekre.

(5) Az NKOH, ahol szükséges, különválasztja a kötelezettségeket és a felelősségeket a nem megengedett módosítási lehetőségek, a véletlen vagy szándékos visszaélések, valamint az információk vagy szolgáltatások nem megfelelő felhasználási lehetőségének csökkentése érdekében.

60. §

Hibajavítás

(1) Az NKOH azonosítja, elektronikus úton jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit. Az üzemeltető telepítés előtt teszteltetti a hibajavítással kapcsolatos szoftverfrissítéseket a feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából. Az üzemeltető a biztonságkritikus szoftvereket a frissítésük kiadását követő 30 napon belül telepíti vagy telepíttetti, majd a konfigurációkezelés folyamata alapján frissíti a konfigurációs adatbázist.

(2) Az üzemeltető által a szoftverek verzióváltásaival, illetve a kiadott hiba és hibajavítási közleményekkel kapcsolatban a következők szerint ját el:

a) a hibajavító csomagokat (service pack) ellenőrzött körülmények között telepíti,

b) jelentős szoftverváltozatok bevezetésénél az előző változatról olyan mentést készít, amely alkalmas a működőképes rendszer állapot visszaállítására.

(3) A szoftverek ellenőrzéséért az üzemeltető felelős.

61. §

Kártékony kódok elleni védelem

(1) A vírusvédelmi rendszer megfelelő működéséért az üzemeltető felelős. A vírusvédelemmel kapcsolatban megfogalmazott általános követelmények az alábbiak:

(2) Az üzemeltető gondolkodik arról, hogy minden Microsoft Windows operációs rendszerrel rendelkező, vagy más vírusok által veszélyeztetett informatikai eszközre vírusvédelmi rendszer legyen telepítve.

(3) A vírusvédelmi rendszernek biztosítania kell:

c) a rendszeres vírusadatbázis frissítést a vírusvédelmi rendszer minden elemén,

d) a központi menedzselhetőséget,

e) azon gyanúsnak ítélt ill. kártékonykódra hasonlító jelsorozatok (nem írtható vírusok) karanténba helyezését, melyek biztonságos eltávolítása nem lehetséges,

f) a vírusfertőzésekről, illetve fertőzött állományok kezelésének naplózását a naplózásra vonatkozó előírások betartásával.

(4) Az NKOH munkaállomásaira telepített vírusvédelmi rendszer beállítási szabályai:

a) a munkaállomáshoz csatlakoztatott tetszőleges adathordozó (pl.: USB diszk), a csatlakozás pillanatában legyen teljes körűen ellenőrizve (on-demand ellenőrzés);

b) a vírusvédelmi rendszer folyamatosan ütemezetten ellenőrzi a munkaállomásokat (on-access ellenőrzés);

c) a vírusvédelmi rendszer épüljön be az elektronikus levelező rendszerbe, minden állomány letöltés és feltöltés előtt végezze el a vírusellenőrzést, csatolt állományok esetében is;

d) a vírusvédelmi rendszert a felhasználó ne kapcsolhassa ki, beállításait ne változtathassa meg.

(5) Az NKOH-n kívülről hozott vagy visszahozott illetve NKOH-n belüli, de antivírus programmal el nem látott gépről érkező adathordozót használatba vétel előtt antivírus programmal ellenőrizni kell.

(6) Az elektronikus levelekkel terjedő vírusok elleni védekezésül az üzemeltető a szerveren vírusszűrőt üzemeltet. A vírust tartalmazó leveleket leggyakrabban a levél feladójaként megjelölt személy tudta nélkül maga a vírus adja fel, ezt a körülményt kihasználva a védekezés hatékonysága a feladó hitelességének ellenőrzésével jelentősen növelhető. Ezért a bejövő e-mail-hez mellékletként csatolt állományt megnyitni, illetőleg programot futtatni csak akkor szabad, ha a címzett előzőleg a feladó valódiságáról (pl. az üzenettörzs alapján) meggyőződött.

(7) Vírusfertőzés észlelése esetében a vírusvédelmi rendszer azt automatikusan eltávolítja, vagy amennyiben ez nem sikerült, akkor karanténba helyezi. Amennyiben az ellenőrzéskor egy dokumentumról vagy programról kiderül, hogy vírussal fertőzött,

akkor azt a fertőzöttség megszüntetéséig nem használható. Amennyiben a vírust nem sikerül eltávolítani, úgy azt a fertőzött dokumentum illetve program törlésével kell megsemmisíteni.

(8) Az NKOH-n kívülről csak a feladatellátásához szükséges adathordozókat szabad behozni, és az (5) bekezdésben meghatározott ellenőrzés után használni.

(8) Az üzemeltető vírusvédelmi rendszer-üzemeltetési tevékenységével szemben támasztott informatikai biztonsági követelmények a következők:

a) a vírusvédelmi rendszer folyamatos üzemeltetése, felügyelete, rendszeres karbantartása, frissítések végrehajtásának ellenőrzése, valamint javaslatok előkészítése a vírusvédelmi rendszer továbbfejlesztésére,

b) a legfrissebb vírusok megjelenésével kapcsolatos hírek nyomon követése, szükség esetén megelőző védelemre javaslat tétel az NKOH felé.

c) fertőzések kezelése, káresemény bekövetkezése esetén részvétel a kárenyhítésben, tevékeny szerep a sérült informatikai eszközök működőképességének biztosításában.

62. §

Az elektronikus információs rendszer felügyelete

(1) Az NKOH az üzemeltető közreműködésével:

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

b) azonosíttatja az elektronikus információs rendszer jogosulatlan használatát;

c) felügyeleti eszközöket alkalmaztat a meghatározott alapvető információk gyűjtésére; és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;

d) biztosítja a behatolás-felügyeleti eszközökből nyert információk védelmét a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

e) erősítteti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;

f) évente biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek.

63. §

Biztonsági riasztások és tájékoztatások

(1) Az IBF folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket továbbá folyamatosan figyelemmel kíséri a Hatóságtól érkező értesítéseket. Az IBF szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, melyet eljuttat az NKOH kapcsolattartójához.

(2) Az IBF kialakítja és működteti az Ibtv-ben meghatározott biztonsági esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel továbbá biztosítja a megfelelő ellenintézkedések és válaszlépések megtételét.

64. §

A kimeneti információ kezelése és megőrzése

(1) Az NKOH az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

XXI. NAPLÓZÁS ÉS MONITOROZÁS

65. §

(1) Az NKOH az elszámoltathatóság és auditálhatóság biztosítása érdekében a Logikai védelmi intézkedések elnöki utasításban meghatározott naplózási eljárásrendben meghatározottak szerint olyan regisztrálási és naplózási rendszert alakít ki, mely alapján utólag meg lehet állapítani a rendszer biztonságát érintő eseményeket. Az NKOH az üzemeltető közreműködésével gondoskodik a biztonsági naplók és a jegyzőkönyvek archiválásáról.

XXII. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

66. §

(1) Az NKOH jelen a Logikai védelmi intézkedések elnöki utasításban meghatározott rendszer- és kommunikációvédelmi eljárásrend dokumentált kihirdetésével és megvalósításával biztosítja a folyamat elvárt működését és ellenőrizhetőségét.

(2) Az informatikai rendszer megfelelő működésének biztosítása érdekében az NKOH hálózatának rendelkezésre állása és biztonságos működése elengedhetetlen. A hálózat biztonságának megteremtése és fenntartása érdekében az NKOH-nál az üzemeltető ellenőrzéseket hajt végre:

a) a fizikai hálózat állapotának és sértetlenségének folyamatos ellenőrzésére,

b) a tűzfal folyamatos menedzselése, a tűzfalon keresztül lebonyolódó hálózati forgalom ellenőrzésére, behatolási kísérletek figyelemmel kísérésére.

(3) Az üzemeltető az NKOH informatikai rendszere és az internet között, határvédelmi technikai megoldásokkal biztosítja a biztonság megfelelő szinten tartását.

(4) Ún. demilitarizált zónákban kell elhelyezni azokat az informatikai eszközöket (szerver, védelmi eszközöket, stb.), melyeknek mind az Internet felöl, mind a belső hálózat felöl, kiemelt védelmet kell biztosítani.

(5) A határvédelmi eszközöknek (tűzfal, IDS) meg kell határozni az optimális életciklusát, melyen belül még megfelelő védelmet nyújt. A megállapított életciklus leteltével a határvédelmi eszköz fejlesztése szükséges.

(6) Az életcikluson belül a határvédelmi eszközök biztonsági frissítéseit rendszeresen el kell végezni.

(7) Biztosítani kell, hogy a határvédelmi eszközökhöz csak az üzemeltető férjen hozzá.

(8) A határvédelmi eszközökön minden kritikus tevékenységet naplózni kell.

(9) A határvédelmi eszközöket rendszeresen monitorozni kell. A monitorozás eredményét minden esetben vissza kell csatolni, ha szükséges fejlesztést, vagy szabályozást kell végrehajtani.

(10) A határvédelem dokumentációját úgy kell tárolni, hogy az indokolatlan hozzáférés, illetve az illetéktelen kezekbe jutásuk elkerülhető legyen.

(11) Az NKOH tevékenységének ellátása során az NKOH szervezetén belüli, valamint az NKOH és a harmadik fél közötti információ átvitel az NKOH ügymenetének szabályai szerint, a vonatkozó szerződéseknek vagy jogszabályi előírásoknak megfelelően, jelen IBSZ előírásainak betartása mellett történik.

(12) Az információ átvitel során az NKOH a szellemi jogok védelmét, a titoktartási megállapodások rögzítését, betartását, az információ védelmét elsődleges szempontnak tartja. Amennyiben szükséges, szerződésben rögzíti az ellenőrzési és egyéb felelősségeket, az értesítések rendjét, a szükséges biztonsági feltételeket. A szerződéskötések rendjét a beszerzési szabályzat tartalmazza.

(13) Az információk védelmét, sértetlenségét biztosító titkosítást - kriptográfiát - az NKOH minimálisan alkalmazza, a Központosított Közbeszerzési Portál üzemeltetése https protokollon keresztül történik.

(14) Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök, így kamerák és mikrofonok távoli aktiválását, kivéve, ha az NKOH engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

Függelékek jegyzéke:

1. számú függelék: Az elektronikus információs rendszerek biztonsági osztályba való sorolása
2. számú függelék: Az elektronikus információs rendszerek nyilvántartása
3. számú függelék: Biztonsági incidens jelentése és kivizsgálása

Az elektronikus információs rendszerek biztonsági osztályba való sorolása

A rendszer megnevezése	Biztonsági besorolása	A rendszer alapfeladata	A rendszer által biztosított szolgáltatások
Központosított Közbeszerzési Portál	3	Központosított közbeszerzés	Központosított közbeszerzéshez regisztráció, éves összesített beszerzési terv és szponzorációs költségkeretterv rögzítése, beszerzési igény, valamint szponzorációra vonatkozó igény rögzítése, beszerzési igények valamint szponzorációra vonatkozó igények elbírálása, szerződések feltöltése
Iktató, KIR3	3	iktatás	iktatás, e-ügyintézés, hivatali kapu

2. számú függelék a ...../2020. (.....) NKOH utasításhoz

Az elektronikus információs rendszerek nyilvántartása

Információs rendszer komponensei	alapfeladat	biztosított szolgáltatás	licensz szám	felügyelő személy (személy azonosító és elérhetőségi adat)		rendszert szállító, fejlesztő, karbantartó szervezet	kapcsolattartó személy (személy azonosító és elérhetőségi adat)	

3. számú függelék a ..../2020. (.....) NKOH utasításhoz

Biztonsági incidens jelentése és kivizsgálása

Incidens időpontja:			
Incidens ügyintézője, beosztása:			
Érintett rendszer:			
Bejelentő neve, beosztása:			
Biztonsági incidens rövid leírása:			
Javító és helyesbítő intézkedés rövid leírása:			
A bejelentés prioritása:	☐ Alacsony	☐ Közepes	☐ Magas
További kivizsgálást igényel-e:	☐ Igen ☐ Nem		
A bejelentés lezárása:			

Kelt: , 20 .....

.....
Bejelentő/Ügyintéző

.....
Informatikai biztonsági felelős