A nemzeti fejlesztési miniszter

…../2013. (... ...) NFM rendelete

az elektronikus információbiztonsággal és az egyes elektronikus információs rendszerekkel kapcsolatos technológiai követelményekről

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (2) bekezdés a) pontjában kapott felhatalmazás alapján,
az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről szóló 212/2010. (VII. 1.) Korm. rendelet 84. § j) pontjában meghatározott feladatkörömben eljárva,
az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről szóló 212/2010. (VII. 1.) Korm. rendelet 2. § (1) bekezdés c) pontjában, valamint a 12. § l) pontjában meghatározott feladatkörében eljáró közigazgatási és igazságügyi miniszterrel egyetértésben
a következőket rendelem el.

1. §

(1) Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 5 és 6. §-ának végrehajtása érdekében az érintett szervezetnek – ideértve az Ibtv. 11. § (1) bekezdés k) - l) pontja szerinti közreműködőt is – az 1. mellékletében előírt adminisztratív, fizikai és logikai rendelkezéseket kell megvalósítani, a 2. számú melléklete szerinti, az érintett szervezet elektronikus információs rendszerének biztonsági besorolásához, valamint az elektronikus információs rendszerrel rendelkező szervezet biztonsági szintjéhez kapcsolódóan.

(2) Az 1. mellékletben írt bármely követelményt, elvárást és feltételt az Ibtv. hatálya alá tartozó érintett szervnek azon elektronikus információs rendszerek tekintetében, olyan mértékig kell teljesíteni, amely mértékig az adott elektronikus információs rendszer tekintetében kapott jogosultságai birtokában arra képes.

(3) Ha az érintett szervezet az elektronikus információs rendszere tekintetében olyan – felügyeleti – jogosultságokkal rendelkezik, amelyek birtokában más szervezet adott elektronikus információs rendszeren történő tevékenységét biztonsági szempontból befolyásolni, irányítani tudja:

a) az 1. számú mellékletben írt bármely követelményt, elvárást és feltételt – jogosultsága mértékéig – a többi, az adott elektronikus információs rendszeren tevékenységet végző szervezet tekintetében is érvényesítenie kell,

b) az 1. számú mellékletben írt bármely követelményt, elvárást és feltételt úgy kell érvényesíteni a többi, az adott elektronikus információs rendszeren tevékenységet végző (kapcsolódó) szervezet tekintetében, hogy a követelmények, feltételek és

elvárások a kapcsolódó szervezet elektronikus információbiztonsággal kapcsolatos eljárásrendjébe az adott rendszer tekintetében beépülhessenek.

2. §

Az Ibtv. 7-8. § végrehajtása érdekében az elektronikus információs rendszerét az érintett szervezetnek a 3. mellékletben foglaltak szerint kell biztonsági osztályba sorolni.

3. §

Az Ibtv. 9-10. § végrehajtása érdekében az elektronikus információs rendszerrel rendelkező, érintett szervezet a 4. mellékletben foglaltak szerint végzi el a biztonsági szintbe sorolást.

4. §

Az Ibtv. 11. § (2)-(3) bekezdés végrehajtása érdekében a Nemzeti Távközlési Gerinchálózat tekintetében az 5. mellékletben foglaltakat kell alkalmazni.

5. §

Ez a rendelet a kihirdetését követő napon lép hatályba.

Budapest, 2013. augusztus „… .”

Németh Lászlóné
nemzeti fejlesztési miniszter

Egyetért:

Dr. Navracsics Tibor
közigazgatási és igazságügyi miniszter

1. melléklet a .../2013. (... ...) NFM rendelethez

AZ ADMINISZTRATÍV, FIZIKAI ÉS LOGIKAI BIZTONSÁGI KÖVETELMÉNYEK

I. ELTÉRÉSEK

Az érintett szervezetnek az alábbi lehetséges eltérésekkel és helyettesítő intézkedésekkel kell, illetve lehet teljesítenie a védelmi intézkedés katalógusban meghatározott minimális követelményeket a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával, a mellett, hogy az érintett szervre érvényes minden kötelezettséget figyelembe kell venni.

I. 1. Működtetéssel, környezettel kapcsolatos eltérések:

A működtetési környezet jellegétől függő biztonsági intézkedések csak akkor alkalmazandók, ha az elektronikus információs rendszert az intézkedéseket szükségessé tevő környezetben használják.

I. 2. A fizikai infrastruktúrával kapcsolatos eltérések:

A szervezeti létesítményekkel kapcsolatos biztonsági intézkedések (zárak, őrök, környezeti paraméterek: hőmérséklet, páratartalom stb.) csak a létesítmény azon részeire alkalmazandók, amelyek közvetlenül nyújtanak védelmet vagy biztonsági támogatást az elektronikus információs rendszernek vagy kapcsolatosak azzal (ideértve a rendszerelemeket is, mint például e-mail, web szerverek, szerver farmok, adatközpontok, hálózati csomópontok, határvédelmi eszközök és kommunikációs berendezések).

I. 3. A nyilvános hozzáféréssel kapcsolatos eltérések:

A nyilvánosan hozzáférhető információkra vonatkozó biztonsági intézkedéseket körültekintően kell számba venni, és végrehajtani, mivel a vonatkozó intézkedés katalógus rész egyes biztonsági intézkedései (például azonosítás és hitelesítés, személyi biztonsági intézkedések) nem alkalmazhatók az elektronikus információs rendszerhez nyilvános interfészeken keresztül hozzáférő felhasználókra.

I. 4. Technológiai eltérések:

A specifikus technológiára (például vezeték nélküli kommunikáció, kriptográfia, PKI) vonatkozó biztonsági intézkedések csak akkor alkalmazandók, ha ezeket a technológiákat használják az elektronikus információs rendszerben vagy előírják ezek használatát.

A biztonsági intézkedések az elektronikus információs rendszer csak azon komponenseire vonatkoznak, amelyek az intézkedés által megcélzott biztonsági képességet biztosítják vagy támogatják, és az intézkedés által csökkenteni kívánt lehetséges kockázatok forrásai.

I. 5. Biztonsági politikával, szabályozással kapcsolatos eltérések:

A tervezett vagy már működtetett elektronikus információs rendszerekre alkalmazott biztonsági intézkedések kialakítása során figyelembe kell venni a rendszer célja által meghatározott vonatkozó törvényi, jogszabályi hátteret, funkciót is.

I. 6. A biztonsági intézkedések bevezetésének fokozatosságával kapcsolatos eltérések:
A biztonsági intézkedések fokozatosan vezethetők be az intézkedés megvalósításának határáig és szigorúságáig. A fokozatosságot a védendő elektronikus információs rendszerek biztonsági kategorizálása alapján lehet felállítani.

I. 7. A biztonsági célokhoz kapcsolódó eltérések:
Azok a biztonsági intézkedések, amelyek kizárólagosan támogatják a bizalmasság, sértetlenség és rendelkezésre állást, visszasorolhatók (vagy módosíthatók, kivehetők, ha alacsonyabb szinten nincsenek meghatározva) alacsonyabb szintre, ha ez az alacsonyabb szintű besorolás:

a) összhangban van a vonatkozó bizalmasságra, sértetlenségre vagy rendelkezésre állásra vonatkozóan az úgynevezett „high water mark” elv alkalmazása előtt megállapított biztonsági szinttel, amely elv az információ biztonság szempontjából azt jelenti, hogy a legmagasabb biztonsági célhoz kell hangolni minden elemet;
b) a „high water mark” elv alkalmazásával az eredeti bizalmassági, sértetlenségi és rendelkezésre állási biztonsági célokat meghaladóan magasabb biztonsági intézkedés szinten történt, és ez nem szükséges a költség-hatékony, kockázat alapú biztonsági intézkedések szempontjából;
c) a szervezetre végrehajtott kockázat elemzés szerint indokolható;
d) nem befolyásolja a biztonsági szempontból fontos információkat az elektronikus információs rendszeren belül.

II. HELYETTESÍTŐ BIZTONSÁGI INTÉZKEDÉSEK

II. 1. A helyettesítő biztonsági intézkedés olyan eljárás, amelyet az érintett szervezet a reá irányadó biztonsági szinthez tartozó biztonsági intézkedés helyett alkalmazni kíván, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, illetve a helyettesített intézkedéssel egyenértékű módon biztosít minden külső, belső követelménynek (például törvényeknek) való megfelelést.

II. 2. Egy elektronikus információs rendszer esetén a szervezet az alábbi feltételek teljesülése esetén alkalmazhat helyettesítő intézkedést:

a) ha az elektronikus információs rendszerek biztonságára vonatkozó szabványokban, vagy hazai ajánlásokban fellelhető helyettesítő intézkedést választja, vagy ha ezekben nincs megfelelő helyettesítő intézkedés, akkor a szervezet kivételesen alkalmazhat egy, az adott helyzetben megfelelő helyettesítő intézkedést;

b) a helyettesítő intézkedések kiválasztásánál a szervezetnek törekednie kell arra, hogy a védelmi intézkedés katalógusból válasszon intézkedést, a szervezet által meghatározott helyettesítő intézkedéseket csak végső esetben szabad használni, amennyiben a biztonsági intézkedések katalógusa nem tartalmaz az adott viszonyok között alkalmazható intézkedést;
c) a vonatkozó szabályozásában be kell mutatnia, hogy a helyettesítő intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, illetve védelmi szintjét, és miért nem használhatók a vonatkozó alapkészlet biztonsági intézkedései;
d) a c) pont szerinti indoklás részletezettségének és szigorúságának az elektronikus információs rendszerre megállapított biztonsági szintnek megfelelőnek kell lennie;
e) a szervezet felméri és a kockázatkezelési eljárási rendnek megfelelően elfogadja a helyettesítő intézkedés alkalmazásával kapcsolatos kockázatot;
f) A helyettesítő biztonsági intézkedések alkalmazását dokumentálni kell, és az eljárási rendnek megfelelően az érintett személlyel, vagy szerepkörrel jóvá kell hagyatni.

III. VÉDELMI INTÉZKEDÉS KATALÓGUS

(Magyarázat: a főfeladat mellett mozaikszó a főfeladat rövidített megnevezése, a feladat melletti szám az adott feladat sorszáma.)

III. 1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

SZERVEZETI SZINTŰ ALAP FELADATOK (AL)

AL 1. Informatikai biztonságpolitika
Az érintett szervezet:
a) megfogalmazza, az érintett szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az informatikai biztonságpolitikát;
b) belső szabályzóban, vagy magában az informatikai biztonságpolitikáról szóló dokumentumban meghatározza a biztonságpolitika felülvizsgálatának és frissítésének gyakoriságát.
Elvárás:
1. meg kell határozni azokat az okokat, melyeknél fogva a kiberbiztonság fontos a szervezet számára, így különösen a biztonsági célok meghatározása, az informatikai biztonságpolitikai szervezeti szempontú alapelveinek bemutatása;
2. be kell mutatni az érintett szervezet vezetői beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítására és támogatására;
3. ki kell fejteni az érintett szervezetben alkalmazott biztonsági alapelveket és megfelelőségi követelményeket;

AL 2. Informatikai biztonsági stratégia
Az érintett szervezet:
a) megfogalmazza, az érintett szervezetre érvényes követelmények szerint

dokumentálja, és a szervezeten belül kihirdeti az informatikai biztonsági stratégiát, amely kifejti az informatikai biztonságpolitikában biztonsági célok megvalósításának módszerét, eszközrendszerét, ütemezését;
b) belső szabályzóban, vagy magában az informatikai biztonsági stratégiáról szóló dokumentumban meghatározza a biztonsági stratégia felülvizsgálatának és frissítésének gyakoriságát;
c) gondoskodik arról, hogy az informatikai biztonsági stratégia jogosulatlanok számára ne legyen megismerhető, illetve módosítható.
Elvárás:
1. A stratégia rövid, közép és hosszú távú célokat tűz ki.
2. A stratégia illeszkedik az érintett szervezet más stratégiáihoz (így különösen a költségvetési és humánerőforrás tervezéshez, tevékenységi kör változáshoz, fejlesztéshez), jövőképéhez.

AL 3 Informatikai biztonsági szabályzat
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;
b) belső szabályzóban, vagy magában az informatikai biztonsági szabályzatról szóló dokumentumban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;
c) gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, illetve módosítható.
Elvárás:
1. az informatikai biztonsági szabályzatban meg kell határozni a
- célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően esetleg területi) hatályát,
- az elektronikus információbiztonsággal kapcsolatos szerepköröket,
- a szerepkörhöz rendelt tevékenységet,
- a tevékenységhez kapcsolódó felelősséget,
- az információbiztonság szervezetrendszerének belső, illetve szervezet egészének együttműködését;

2. az informatikai biztonsági szabályzat a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza akár külön függelékekben, akár egységes szerkezetben:
- kockázatelemzést (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz),
- biztonsági helyzet-, és eseményértékelés eljárási rendjét,
- rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzést (amennyiben Az érintett szervezet ilyet végez, vagy végezhet),
- biztonsággal kapcsolatos tervezést (például: beszerzés, fejlesztés, eljárásrendek kialakítását),
- fizikai és környezeti védelem szabályait, jellemzőit,
- az emberi erőforrásokban rejlő veszélyek megakadályozását (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.)

- az informatikai biztonság tudatosítására irányuló tevékenységet és képzést, szervezet összes érintett tagja tekintetében,
- az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatokat, elvárásokat, jogokat (amennyiben a szervezetnél ez értelmezhető),
- üzlet, vagy üzemmenet folytonosság tervezését (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.),
- az elektronikus információs rendszerek karbantartásának rendjét,
- az adathordozók fizikai és logikai védelmének szabályozását,
- az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárást, illetve a hozzáférés szabályok betartásának ellenőrzését,
- amennyiben a szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelését, az értékelés eredményétől függő eljárások meghatározását,
- az adatok mentésének, archiválásának rendjét,
- a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárást, ideértve a helyreállítást is,
- az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az informatikai biztonságot érintő, szerződéskötés során érvényesítendő követelményeket;

3. meghatározza a biztonsági szintjét, valamint a szervezet összes elektronikus információs rendszerének biztonsági osztályát.

AL 4. Az elektronikus információs rendszerek biztonságáért felelős személy

Az érintett szervezet vezetője az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki:

a) azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel;

b) ellátja a törvény Ibtv. 13 §-ban meghatározott feladatokat.

AL 5. Pénzügyi erőforrások biztosítása

Az érintett szervezet:

a) a költségvetés tervezés, és a beruházások, beszerzések során biztosítja az informatikai biztonsági stratégia megvalósításához szükséges forrásokat, illetve dokumentálja ezen követelmény alá eső kivételeket;

b) biztosítja a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állását.

Elvárás:

A pénzügyi erőforrások tervezése illeszkedik AL 2-höz.

AL 6. Cselekvési terv és mérföldkövei
Az érintett szervezet:
a) cselekvési tervet készít az informatikai biztonsági stratégia megvalósításához, ebben mérföldköveket határoz meg;
b) karbantartja a cselekvési tervet
Elvárás:
Felülvizsgálja és karbantartja a cselekvési tervet és mérföldköveit
1 a szervezet kockázatkezelési stratégiájának és a kockázatokra adott válasz tevékenységeknek az érintett szervezet belső prioritása alapján;
2. ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály Ibtv. 8. § szerinti meghatározásánál hiányosságot állapít meg (ebben az esetben a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetésére koncentrálva);
3. ha a szervezet által meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre az Ibtv. 9. § (2) bekezdésében előírt biztonsági szint (ebben az esetben a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a szervezet számára előírt biztonsági szint elérésére koncentrálva).

AL 7. Az elektronikus információs rendszerek nyilvántartása
Az érintett szervezet:
a) elektronikus információs rendszereiről nyilvántartást készít;
b) folyamatosan aktualizálja a nyilvántartást.
Elvárás:
1. a nyilvántartás minden rendszerre tartalmazza annak alap feladatait,
2. a rendszerek által biztosítandó szolgáltatásokat,
3. tartalmazza az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett szerv kezelésében vannak),
4. a rendszer felett felügyeletet gyakorló személyazonosító és elérhetőségi adatait,
5. a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek azonosító és elérhetőségi adatait.

AL 8. A biztonsági teljesítmény mérése
Az érintett szervezet kifejleszti, felügyeli és értékeli elektronikus információs rendszere biztonsági teljesítményét.

AL 9. Szervezet szintű architektúra
Az érintett szervezet a szervezeti felépítés/szervezeti szintű architektúra kialakításánál figyelembe veszi a szervezet működését befolyásoló kockázati tényezőket.

AL 10. Kockázatkezelési stratégia
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a kockázatkezelési stratégiát;
b) következetesen alkalmazza a kockázatkezelési stratégiát Az érintett szervezet egészére;

c) belső szabályzóban, vagy magában a kockázatkezelési stratégiában szóló dokumentumban meghatározza a kockázatkezelési stratégia felülvizsgálatának és frissítésének gyakoriságát.
Elvárás:
1. a stratégia terjedjen ki Az érintett szervezetnél lehetséges kockázatok felmérésére,
2. a stratégia terjedjen ki a kockázatok kezelésének felelősségére,
3. a stratégia terjedjen ki a kockázatok kezelésének elvárt minőségére.

AL 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;
b) irányítja és kezeli az elektronikus információs rendszer és környezet biztonsági állapotát;
c) egyértelműen meghatározza az információbiztonsággal összefüggő szerep- és felelősség köröket, kijelöli az ezeket betöltő személyeket;
d) integrálja az elektronikus információbiztonsággal engedélyezési folyamatokat Az érintett szervezeti szintű kockázatkezelési eljárásba, kapcsolatban az információbiztonsági szabályzattal.
Elvárás:
1. az elektronikus információbiztonsággal kapcsolatos engedélyezés terjedjen ki minden az érintett szerv hatókörébe tartozó emberi, fizikai és logikai erőforrásra,
2. terjedjen ki minden, a szervezet hatókörébe tartozó szintre és folyamatra.

AL 12 .Tesztelés, képzés és felügyelet
Az érintett szervezet:
Amennyiben ez hatókörébe tartozik, megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárások:
1. kifejlesztését és fenntartását,
2. folyamatos időbeni végrehajtását.
Elvárás:
Felülvizsgálja a tesztelési, képzési és ellenőrzési terveket Az érintett szervezet kockázatkezelési stratégiája és a biztonsági eseményekre a kockázatkezelés alapján definiált reakciók szervezeti prioritása (az események súlyossága) alapján.

AL 13. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel
Az érintett szervezet
a) az alkalmazottak folyamatos oktatásának, képzésének elősegítése;
b) az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása;
c) a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása

érdekében kapcsolatot alakít ki és tart fenn.

KOCKÁZATELEMZÉS (KE)

KE 1. Kockázatelemzési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és Az érintett szervezeten belül kihirdeti a kockázatelemzési eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező kockázatelemzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) belső szabályzóban, vagy magában a kockázatelemzési eljárásrendről szóló dokumentumban meghatározza a kockázatelemzési eljárásrend felülvizsgálatának és frissítésének gyakoriságát.

KE 2. Biztonsági osztályba sorolás
Az érintett szervezet:
a) a jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit az azokról szóló AL 7. nyilvántartás alapján, és meghatározza, hogy azok a vizsgálat elvégzésekor melyik biztonsági osztálynak felelnek meg;
b) rögzíti a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában;
c) vezetője jóváhagyja a biztonsági osztályba sorolást.
Elvárás:
1. a biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni,
2. kapcsolódást kell biztosítani AL 6-hoz.

KE 3. Kockázatelemzés
Az érintett szervezet:
a) végrehajtja a biztonsági kockázatelemzéseket;
b) megállapítja a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy más a KE 1. szerint előírt dokumentumban;
c) a KE 1. szerinti felülvizsgálja a kockázatelemzések eredményét;
d) a KE 1., vagy AL 3. szerint megismerteti a kockázatelemzés eredményét az érintettekkel;
e) amikor jelentős 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;
f) gondoskodik arról, hogy a kockázatelemzési eredmények jogosulatlanok számára ne legyenek megismerhetők.

KE 4. Sebezhetőség vizsgálat
Az érintett szervezet

a) sebezhetőség vizsgálatot végez az elektronikus információs rendszerei, és alkalmazásai tekintetében, amennyiben az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei, valamint a szervezet felkészültsége, a rendelkezésre álló erőforrás lehetővé, illetve azt jogszabály kötelezővé teszi;
b) a szervezet által meghatározott gyakorisággal és/vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sebezhetőség merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban;
c) az eljárást sebezhetőség vizsgálati eszközök és technikák alkalmazásával, vagy külső szervezet bevonásával lehet végezni, és csak azon elektronikus információs rendszerek tekintetében, amelyek a szervezet felügyelete, irányítása alatt állnak;
d) KE 4.1. – KE 4.4. pont szerinti metodikát használja.
Elvárás:
1. kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról,
2. végrehajtja az ellenőrzési listákat és tesztelési eljárásokat,
3. felméri a sebezhetőség lehetséges hatásait,
4. elemzi a sebezhetőség vizsgálatok eredményét,
5. megosztja a sebezhetőség vizsgálatok eredményét a szervezet által meghatározott személyekkel és szerepkörökkel,
6. c) gondoskodik arról, hogy vizsgálati eredmények jogosulatlanok számára ne legyen megismerhetők.

KE 4. 1. Frissítési képesség
Az érintett szervezet olyan sebezhetőség vizsgálati eszközt alkalmaz, melynek sebezhetőség feltáró képessége könnyen bővíthető az ismertté váló sebezhetőségekkel.

KE 4. 2. Frissítés időközönként, új vizsgálat előtt vagy új sebezhetőség feltárását követően
Az érintett szervezet az elektronikus információs rendszerre vizsgált sebezhetőségek körét aktualizálja, az új vizsgálatot megelőzően, vagy a sebezhetőség feltárását követően azonnal.

KE 4. 3. Privilegizált hozzáférés
Az elektronikus információs rendszer privilegizált hozzáférést biztosít az érintett szervezet által kijelölt rendszer elemekhez a sebezhetőség vizsgálat végrehajtásához.

KE 4. 4. Felfedhető információk
Az érintett szervezet meghatározza, hogy egy támadó milyen információkat fedhet fel az elektronikus információs rendszerrel kapcsolatban, majd ezt követően javításokat hajt végre.

TERVEZÉS (TE)

TE 1. Biztonságtervezési eljárásrend

Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező biztonságtervezési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a biztonságtervezési eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságtervezési eljárásrendet.

TE 2. Rendszerbiztonsági terv
Az érintett szervezet, amennyiben az elektronikus információs rendszer tervezése hatókörébe tartozik:
a) az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, amely:
1. összhangban áll a szervezeti felépítésével/szervezeti szintű architektúrájával (AL 9.),
2. meghatározza az elektronikus információs rendszer hatókörét, alap feladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alap funkcióit,
3. meghatározza elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát,
4. meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerrel való kapcsolatait,
5. a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit,
6. meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedésbővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat.
Elvárás:
b) gondoskodik arról, hogy a rendszerbiztonsági tervet az érintett szervezet által meghatározott személyi- és szerepkörök megismerje (ideértve annak változásait is);
c) belső szabályzóban, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felül kell vizsgálni az elektronikus információs rendszer rendszerbiztonsági tervét;
d) frissíteni kell a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
e) elvégzi a TE 2. 1. pont szerintieket;
e) gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, illetve módosítható.

> TE 2. 1. Belső egyeztetés
> Az érintett szervezet tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak nem érintett, saját szervezeti egységeire gyakorolt hatását.

TE 3. Személyi biztonság
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési

jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet (kapcsolat AL 3-al, és AL 11-el);
b) az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozat megtételére szólítja fel a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismert, saját felelősségére betartja;
c) meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályokat;
d) gondoskodik arról, hogy a c) pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a b) pont szerinti eljárás megtörténjen;
e) meghatározza a szervezeten kívüli irányban megvalósuló követelményeket

TE 3. 1. Közösségi oldalak használata

a) Az érintett szervezet viselkedési normája fokozottan tiltja a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;
b) tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak nem kívánt levelezőlisták, stb.);
c) tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.

TE 4. Információbiztonsági architektúra leírás

Az érintett szervezet (amennyiben az hatókörébe tartozik, és amennyiben az más dokumentumban nem kerül meghatározásra, vagy azokból nem következik):
a) elkészíti az elektronikus információs rendszer információbiztonsági architektúra leírását;
b) a szervezet általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja és frissíti az információbiztonsági architektúra leírást;
c) biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben és a beszerzésekben.
Elvárás információbiztonsági architektúra leíráshoz:
1. összegezze az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának a védelmét szolgáló filozófiát, követelményeket és megközelítést,
2. fogalmazza meg, hogy az információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába és hogyan támogatja azt,
3. írja le a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS (RB)

Jelen címben meghatározott eljárásokat abban az esetben kell bevezetni az érintett szervezetnél, amennyiben saját hatókörében informatikai szolgáltatást, vagy

eszközöket (ide nem értve a jellemzően kisebb egyedi értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, illetve azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, illetve az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket) nem szerez be, illetve nem végez, vagy végeztet rendszerfejlesztési tevékenységet. Nem kell a fejlesztések tekintetében előírt követelményeket alkalmazni, amennyiben azok a kereskedelmi forgalomban kapható szoftverek szolgáltatásainak kihasználásával jönnek létre.

RB 1. Beszerzési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a beszerzési eljárásrendet, mely a szervezet elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a beszerzési eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.

RB 2. Erőforrás igény felmérés
Az érintett szervezet:
a) az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, dokumentálja és biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás, vagy költségvetés tervezés részeként;
b) elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás, vagy költségvetési tervezési dokumentumaiban.

RB 3. A rendszer fejlesztési életciklusa
Az érintett szervezet:
a) elektronikus információs rendszereit a rendszer teljes életútjára tekintettel kezeli, amelynek minden életciklusában figyelemmel van az informatikai biztonságra;
b) a fejlesztési életciklus egészére meghatározza és dokumentálja az információ biztonsági szerepköröket és felelősségeket;
c) meghatározza, és a szervezetre érvényes szabályok szerint kijelöli az információ biztonsági szerepköröket betöltő, felelős személyeket.
Elvárás:
Egy rendszer életciklus szakaszait a következők szerint kell meghatározni:
1. követelmény meghatározás,
2. fejlesztés/beszerzés,
3. megvalósítás/értékelés,
4. üzemeltetés és fenntartás,
4. kivonás (archiválás, megsemmisítés).

RB 4. Beszerzések
Az érintett szervezet az elektronikus információs rendszerre, rendszer elemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként határozza meg az alábbiakat:
a) funkcionális biztonsági követelmények;
b) garanciális biztonsági követelmények (pl. a biztonságkritikus termékekre elvárt garanciaszint);
c) a biztonsággal kapcsolatos dokumentációs követelmények;
d) a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények;
e) az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírások;
f) elfogadási kritériumok.

RB 4 (1) A védelmi intézkedések funkcionális tulajdonságai
Az érintett szervezet szerződéses követelményként határozza meg a fejlesztő, szállító számára, hogy hozza létre és bocsássa az érintett szervezet rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

RB 4 (2) A védelmi intézkedések terv- és megvalósítási dokumentációi
Az érintett szervezet szerződéses követelményként határozza meg a fejlesztő, szállító számára, hogy hozza létre és bocsássa a szervezet rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas, és alacsony szintű biztonsági tervet, illetve – amennyiben azzal a szállító rendelkezik – a forrás kódot és futtatókörnyezetet

RB 4 (3) Funkciók – protokollok – szolgáltatások
Az érintett szervezet szerződéses rendelkezésként követelje meg a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában határozza meg a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

RB 5. Az elektronikus információs rendszerre vonatkozó dokumentáció
Az érintett szervezet:
a) amennyiben az hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amelynek tartalmaznia kell:
1. a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését;
2. a biztonsági funkciók hatékony alkalmazását és fenntartását;
3. a konfigurációval és az adminisztratív funkciók használatával kapcsolatos ismert sérülékenységeket;
b) megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszer elemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amelynek tartalmaznia kell:

1. a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,
2. a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos használatának módszereit,
3. a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;
c) amennyiben a szervezetnek az a) – b) pont szerinti dokumentációk nem állnak rendelkezésére dokumentációval alátámasztható módon intézkedéseket tesz ezek megszerzésére;
d) c) gondoskodik arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori – dokumentáció jogosulatlanok számára ne legyen megismerhető, illetve módosítható;
e) gondoskodik a dokumentációknak a szervezet által meghatározott szerepköröket betöltő személyek által, illetve a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

RB 6. Biztonságtervezési elvek
Az érintett szervezet – amennyiben az adott információs rendszer specifikálása hatókörébe tartozik – biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.

RB 7. Külső elektronikus információs rendszerek szolgáltatásai
Az érintett szervezet:
a) szerződéses kötelezettségként követeli meg, hogy a külső – nem az érintett szervezet által üzemeltetett, hanem annak szolgáltatásait szerződés alapján igénybe vett – elektronikus információs rendszerek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek;
b) meghatározza és dokumentálja a szervezet felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;
c) folyamatosan ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

> RB 7. 1. Funkciók, portok, protokollok, szolgáltatások
> Az érintett szervezet megköveteli, hogy a szolgáltató határozza meg a szolgáltatások igénybe vételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

RB 8. Fejlesztői változáskövetés
Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:
a) vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;
b) dokumentálja, kezelje és ellenőrizze a változtatások sértetlenségét;
c) csak a szervezet által jóváhagyott változtatásokat hajtsa végre az elektronikus

információs rendszeren, rendszer elemen vagy rendszerszolgáltatáson;
d) dokumentálja a szervezet által jóváhagyott változtatásokat, illetve ezek lehetséges biztonsági hatásait;
e) kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit a szervezet által meghatározott személyeknek.

RB 9. Fejlesztői biztonsági tesztelés
Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője:
a) készítsen biztonságértékelési tervet és hajtsa végre az abban foglaltakat;
b) hajtson végre (a fejlesztéshez illeszkedő módon egység, integrációs, rendszer, regressziós tesztelést, és ezt értékelje ki a szervezet által meghatározott lefedettség és mélység mellett;
c) bizonyítsa, hogy végrehajtotta a biztonságértékelési tervben foglaltakat és ismertesse a biztonsági tesztelés és értékelés eredményeit;
d) javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

RB 10. A védelem szempontjainak érvényesítése a beszerzés során
Az érintett szervezet az informatikai biztonságpolitikájában lefektetett elveknek megfelelően védi az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés alkalmazásából adódó kockázatok ellen.

RB 11. Fejlesztési folyamat, szabványok és eszközök
Az érintett szervezet:
a) megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen;
b) a szervezet által meghatározott biztonsági követelményeknek való megfelelés érdekében szervezet által meghatározott gyakorisággal a fejlesztő áttekinti a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.
Elvárás hogy a dokumentált fejlesztési folyamat:
1. kiemelten kezeli a biztonsági követelményeket,
2. meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket,
3. dokumentálja a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat,
4. dokumentálja és kezelje a változtatásokat, továbbá biztosítsa ezek engedély nélküli megváltoztatás elleni védelmét.

RB 12. Fejlesztői oktatás
Az érintett szervezet oktatási kötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára, hogy a szervezet által kijelölt személyek (elsősorban adminisztrátorok) és biztonsági felelősök a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák.

RB 13. Fejlesztői biztonsági architektúra és tervezés

Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre amely:
a) illeszkedik a szervezet biztonsági architektúrájához és támogatja azt;
b) leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között;
c) bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.

BIZTONSÁGI ELEMZÉS (BE)

BE-1 Biztonságelemzési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a biztonságértékelési eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező biztonságértékelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a biztonságértékelési eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.

BE-2 Biztonsági értékelések
Az érintett szervezet:
a) készítsen biztonságértékelési tervet,
b) meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, a bevezetett intézkedések működőképességének kontrollja, tervezettnek megfelelő működés, a biztonsági követelményeknek való megfelelőség ellenőrzése érdekében;
c) elkészíti a biztonságértékelés eredményét összefoglaló jelentést;
d) gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek a szervezet által meghatározott szerepköröket betöltő személyek által, illetve a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.
Elvárás, hogy a biztonsági értékelés tartalmazza:
1. az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedések,
2. biztonsági ellenőrzések eredményességét meghatározó eljárásrendek,
3. értékelési környezetet, értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

BE 2. 1. Független értékelők
Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére.

BE 2. 2. Speciális értékelés
Az érintett szervezet a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélkül sebezhetőség vizsgálatot; rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi

fejlesztésű szoftverelemek forráskód elemzését, a szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.

BE 3. Az elektronikus információs rendszer kapcsolódásai
Az érintett szervezet:
a) belső engedélyezési eljárást folytat le, amikor felmerül az igény, hogy elektronikus információs rendszere kapcsolódjon más elektronikus információs rendszerekhez;
b) dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

BE-3 (1) Külső kapcsolódásokra vonatkozó korlátozások
Az érintett szervezet a külső elektronikus információs rendszerekhez való kapcsolódásokhoz informatikai biztonsági szabályzatában szabályrendszert állít fel, és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése; vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

BE 4. Cselekvési terv
Az érintett szervezet:
a) a törvény 8. § (5) alattiaknak megfelelően cselekvési tervet készít, ha Az érintett szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;
b) a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;
c) frissíti a meglévő cselekvési tervet a szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

BE 5. Folyamatos ellenőrzés
Az érintett szervezet folyamatba épített ellenőrzést/ellenőrzési tervet hajt végre, amely tartalmazza:
a) az ellenőrizendő mérőszámokat;
b) az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;
c) az érintett szervezet ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;
d) a mérőszámok megfelelőségét;
e) az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;
f) a szervezet (vagy szervezeti egység) reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;
g) a szervezet által meghatározott gyakorisággal. gondoskodik arról, hogy az elemzési adatokat az érintett szervezet által meghatározott személyi- és szerepkörök megismerjék (ideértve azok változásait is).

BE 5. 1. Független értékelés

Az érintett szervezet lehetőleg független értékelőket vagy értékelő csoportokat alkalmaz az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére.

BE 6. Áthatolhatósági (penetrációs) tesztelés
Az érintett szervezet áthatolhatósági (penetrációs) tesztelést végez, meghatározott gyakorisággal, a szervezet által kijelölt elektronikus információs rendszerre vagy rendszer elemekre.

BE 7. Belső rendszer kapcsolatok
Az érintett szervezet:
a) belső engedélyezési eljárást folytat le, amikor felmerül az igény, hogy elektronikus információs rendszere kapcsolódjon másik saját elektronikus információs rendszerekhez;
b) dokumentálja az egyes belső kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ – SZEMÉLY – BIZTONSÁG (SZ)

Minden, a személybiztonsággal kapcsolatos eljárás, vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a jelen fejezet felé irányuló elvárásait a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötés során kell, mint kötelezettséget érvényesíteni (ideértve szabályzatok, eljárásrendek megismerése és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot)

SZ 1. Személybiztonsági eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a személybiztonsági eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező személybiztonsági követelményeket tartalmazza, és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a személybiztonsági eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a személybiztonsági eljárásrendet.

SZ 2. Munkakörök, feladatok biztonság szempontú besorolása
Az érintett szervezet:
a) minden szervezeti munkakört, vagy szervezethez kapcsolódó feladatot besorol;
b) meghatározza a fontos és bizalmas munkaköröket betöltő személyekre elvárt nemzetbiztonsági ellenőrzés típusát („A”, „B” vagy „C”); .
c) rendszeresen felülvizsgálja és frissíti a munkakörök minősítését besorolását

SZ 3. A személyek ellenőrzése
Az érintett szervezet:
a) az elektronikus információs rendszerhez hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a betöltendő szervezeti munkakör besoroláshoz szükséges feltételekkel rendelkezik-e;
b) fontos és bizalmas munkakör esetén kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést;
c) folyamatosan ellenőrzi az a)-b) pontokban írt feltételek fennállását.

SZ 4. Eljárás jogviszony megszűnésekor
Az érintett szervezet:
a) belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez;
b) megszünteti, illetve visszaveszi a személy egyéni hitelesítő eszközeit;
c) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;
d) visszaveszi a szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
e) megtartja a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;
f) a szervezet által meghatározott módon a jogviszony megszűnéséről értesíti a szervezet által meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.
Elvárás:
1. a szervezet a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik,
2. a jogviszony megszűnésekor fokozott figyelmet kell fordítani arra, hogy a jogviszonyt megszüntető személy esetleges káros tevékenysége megelőzhető legyen.

SZ 4. 1. Automatikus figyelmeztetés
Az érintett szervezet automatikus mechanizmusokat alkalmaz a szervezet által meghatározott szerepköröket betöltő, feladatokat ellátó személyek értesítésére a jogviszony megszűnése esetén.

SZ 5. Az áthelyezések, átirányítások és kirendelések kezelése
Az érintett szervezet:
a) szükség esetén elvégzi a SZ 3. szerinti eljárást;
b) logikai és fizikai hozzáférési engedélyez az újonnan használni kívánt elektronikus információs rendszerhez;
c) szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását, vagy megszüntetését;
d) a szervezet által meghatározott módon a jogviszony változásáról értesíti a szervezet által meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

SZ 6. A szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

Az érintett szervezet:
a) a külső szervezettel kötött megállapodás, szerződés részévé teszi, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos az információbiztonságot érintő szerep- és felelősség köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
b) szerződéses kötelezettségként követelje meg, hogy a külső szervezet feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek;
c) a külső szervezettől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;
d) előírja, hogy ha a külső szervezettől olyan személy lép ki vagy kerül áthelyezésre, aki rendelkezik a szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek;
e) folyamatosan ellenőrzi a külső szervezet személybiztonsági követelményeknek való megfelelését.

SZ 7. Fegyelmi intézkedések
Az érintett szervezet:
a) belső eljárási rendje szerint fegyelmi intézkedést kezdeményez az elektronikus információ biztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;
b) amennyiben az elektronikus információ biztonsági szabályokat nem a szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

TUDATOSSÁG ÉS KÉPZÉS (TK)

TK 1. Képzési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a képzési eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező képzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a képzési eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.

TK 2. Biztonság tudatosság képzés
Az érintett szervezet az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:
a) az új felhasználók kezdeti képzésének részeként;
b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
c) ezen túlmenően a szervezet által meghatározott gyakorisággal.
Elvárás
A biztonság tudatossági képzés az érintett személyeket készítse fel a lehetséges belső

fenyegetések felismerésére.

TK 2. 1. Belső fenyegetés
A biztonság tudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, tudatosítsa jelentési kötelezettségét.

TK 3. Szerepkör, illetve feladat alapú biztonsági képzés
Az érintett szervezet szerepkör, illetve feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek:
a) az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
c) ezen túlmenően a szervezet által meghatározott gyakorisággal.

TK-4 A biztonsági képzésre vonatkozó dokumentációk
Az érintett szervezet:
a) dokumentálja a biztonság tudatosságra vonatkozó alap és szerepkör alapú biztonsági képzéseket;
b) a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi.

III. 2. FIZIKAI VÉDELMI INTÉZKEDÉSEK

FIZIKAI ÉS KÖRNYEZETI VÉDELEM (FK)

Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi rendelkezésekre.
Jelen rendelkezések az adott létesítmény szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.

FK 1. Fizikai védelmi eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre és/vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely szervezet informatikai biztonsági, vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a fizikai védelmi eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.

FK 2. Fizikai belépési engedélyek
Az érintett szervezet:

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

FK 3. A fizikai belépés ellenőrzése
Az érintett szervezet:
a) biztosítja az engedélyesek számára a fizikai belépést, kizárólag a szervezet által meghatározott be-, illetve kilépési pontokon;
b) naplózza a fizikai belépéseket;
c) ellenőrzés alatt tartja a létesítményen belüli, nyilvánosan elérhető helyiségeket;
d) kíséri a látogatókat és figyelemmel követi a tevékenységüket;
e) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
f) nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
g) szervezet által meghatározott gyakorisággal változtatja meg a hozzáférési kódokat és kulcsokat, illetve azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személyt elveszti a belépési jogosultságát.
Elvárás:
1. az egyéni belépési engedélyeket a belépési pontokon ellenőrizni kell,
2. a kijelölt pontokon való átjutást felügyelni kell a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel,
3. fel kell hívni a szervezet tagjainak figyelmét a rendellenességek jelentésére.

> FK 3. 1. Hozzáférés az információs rendszerhez.
> A létesítménybe történő fizikai belépés ellenőrzésén túl engedélyhez köti fizikai belépést az elektronikus információs rendszerekhez, illetve az azokat tartalmazó helyiségekhez is.

FK 4. Hozzáférés az az adatátviteli eszközökhöz és csatornákhoz
Az érintett szervezet ellenőrzi a fizikai belépést az elektronikus információs rendszer adatátviteli eszközeit és kapcsolódási pontjait tartalmazó helyiségekhez, a szervezet által meghatározott biztonsági védelemmel.

FK 5. A kimeneti eszközök hozzáférés ellenőrzése
Az érintett szervezet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek hozzá a kimenethez.

FK 6. A fizikai hozzáférések felügyelete
Az érintett szervezet:

a) ellenőrzi az elektronikus információs rendszereket tartalmazó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra;
b) rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat;
c) azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak;
c) összehangolja biztonság események kezelését a napló átvizsgálások eredményét.

FK 6. 1. Behatolás riasztás, felügyeleti berendezések
Felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.

FK 6. 2. Az elektromos információs rendszerekhez való hozzáférés felügyelete
A létesítménybe való fizikai belépések ellenőrzésén felül külön felügyeli az elektromos információs rendszer egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépéseket.

FK 7. A látogatók ellenőrzése
Az érintett szervezet:
a) meghatározott ideig megőrzi az elektronikus információs rendszereket tartalmazó létesítményekbe történt látogatói belépésekről szóló információkat;
b) azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

FK 7. 1. Automatizált látogatói információkezelés
A szervezet automatizált mechanizmusokat alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez, átvizsgálásához.

FK 8. Áramellátó berendezések és kábelezés
Az érintett szervezet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

FK 9. Vészkikapcsolás
Az érintett szervezet:
a) lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszer elemek áramellátásának kikapcsolására vészhelyzetben;
b) gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről;
c) védi a vészkikapcsolás lehetőségét a jogosulatlan aktivizálástól.

FK 10. Tartalék áramellátás
Az érintett szervezet
a) az elsődleges áramforrás kiesése esetére, a szervezet által végzett tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához és/vagy a hosszú távú tartalék áramellátásra történő átkapcsoláshoz.

FK 10. 1. Hosszú távú tartalék áramellátás a minimálisan elvárt működési képességhez
Az elsődleges áramforrás kiesése esetén biztosítja a hosszú távú tartalék áramellátást az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.

FK 11. Vészvilágítás
Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

FK 12. Tűzvédelem
Az érintett szervezet
Az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

FK 12. 1. Automatikus tűzelfojtás
A személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít.

FK 12. 2. Észlelő berendezések, rendszerek
Elektronikus információs rendszer védelmére olyan tűzjelző berendezést/rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által meghatározott tűzvédelmi felelősnek.

FK 12. 3. Tűzelfojtó berendezések, rendszerek
Az elektronikus információs rendszer védelmére olyan tűzelfojtó berendezést/rendszert alkalmaz, amely aktiválásáról automatikusan jelzést kap az érintett szervezet által meghatározott tűzvédelmi felelős.

FK 13. Hőmérséklet és páratartalom ellenőrzés
Az érintett szervezet
a) az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) szabályozottan elfogadható szinten tartja a hőmérsékletet és páratartalmat;
b) az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) figyeli a hőmérséklet és páratartalom szintjét.

FK 14. Vízkár elleni védelem
Az érintett szervezet

Védi az elektronikus információs rendszert a vízszivárgásokból származó vízkárokkal szemben, biztosítva, hogy a fő elzáró szelepek hozzáférhetőek, megfelelően működnek és a kulcsszemélyek számára ismertek.
Elvárás:
Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során kiemelt figyelmet kell fordítani arra, hogy az a vízkártól védett legyen, akár vízvezetékek kiváltásával, áthelyezésével is.

FK 14. 1. Automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer közelében megjelenő víz észlelésére és a szervezet által meghatározott személyek riasztására.

FK-15 Be és kiszállítás
Az érintett szervezet engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, illetve onnan kivitt információs rendszer elemeket, és nyilvántartást vezet ezekről.

FK-16 Tartalék munkahelyszínek
Az érintett szervezet:
a) meghatározott biztonsági felügyeletet tart fenn a tartalék munkahelyszíneken;
b) értékeli a tartalék munkahelyszínekre vonatkozó biztonsági felügyelet hatásosságát;
c) biztosítja az alkalmazottak számára a biztonsági esemény vagy probléma bejelentési lehetőségét a biztonsági személyzet számára.

FK-17 Az elektronikus információs rendszer elemeinek elhelyezése
Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből] adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

III. 3. LOGIKAI VÉDELMI INTÉZKEDÉSEK

KONFIGURÁCIÓKEZELÉS (KK)

KK 1. Konfigurációkezelési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező konfiguráció kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a fizikai védelmi eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

KK 2. Alap konfiguráció
Az érintett szervezet az elektronikus információs rendszereihez egy-egy alap konfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

KK 2. 1. Áttekintések és frissítések
Az alap konfiguráció frissítését az elektronikus információs rendszer elemek telepítésének és frissítéseinek szerves részeként kell elvégzi.

KK 2. 2. Korábbi konfigurációk megőrzése
Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alap konfigurációját, és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérést.

KK 2. 3. Magas kockázatú területek konfigurálása
a) biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszer elemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják;
b) megfelelő biztonsági eljárásokat kell alkalmazni az a) pont szerinti eszköz belső használatban vonásakor.

KK 2. 4. Automatikus támogatás
Automatikus mechanizmusokat kell alkalmazni az elektronikus információs rendszer naprakész, teljes, pontos, és állandóan rendelkezésre álló alap konfigurációjának a karbantartására.

KK 3. A konfigurációváltozások felügyelete (változáskezelés)
Az érintett szervezet:
a) meghatározza a változáskezelési felügyelet alá eső változás típusokat,
b) meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemet, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.)

c) megvizsgálja a változáskezelési felügyelet elé terjesztett javasolt változtatásokat, majd biztonsági hatásvizsgálatuk figyelembe vételével jóváhagyja, vagy elutasítja azokat,
d) dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket,
e) megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben,
f) visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását.,
g) auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

KK 3. 1. Előzetes tesztelés és megerősítés
A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ez után dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

KK 3. 2. Automatikus támogatás
Automatikus mechanizmusokat kell alkalmazni:
a) az elektronikus információs rendszerben javasolt változtatások dokumentálására;
b) a jóváhagyásra jogosultak értesítésére;
c) a késedelmes jóváhagyások kiemelésére;
d) a még nem jóváhagyott változások végrehajtásának a megakadályozására;
e) az elektronikus információs rendszerben végrehajtott változások teljes dokumentálására;
f) a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.

KK 4. Biztonsági hatásvizsgálat
Az érintett szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásokat az információbiztonságra való hatásuk meghatározása érdekében, még a változtatások megvalósítása előtt.

KK. 4. 1. Elkülönített teszt környezet
A változtatásokat éles rendszerben történő megvalósításuk előtt egy elkülönített teszt környezetben vizsgálja meg, hibákat, sebezhetőségeket, kompatibilitási problémákat és szándékos károkozásra utaló jeleket keresve.

KK 5. A változtatásokra vonatkozó hozzáférés korlátozások
Az érintett szervezet belső szabályozásaiban meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, illetve jóváhagyja azokat, illetve fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.

KK. 5. 1. Automatikus támogatás
Az elektronikus információs rendszerben automatikus mechanizmusokat kell alkalmazni a hozzáférési korlátozások érvényesítése érdekében, az ezzel kapcsolatos tevékenység naplózására.

KK. 5. 2. Felülvizsgálat
Rendszeresen felül kell vizsgálni az elektronikus információs rendszer változtatásait annak megállapítása érdekében, hogy nem történt-e jogosulatlan változtatás.

KK. 5. 3.Aláírt elemek
A szervezet által meghatározott szoftver és firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva, ismert és jóváhagyott tanúsítvány alkalmazásával.

KK 6. Konfigurációs beállítások
Az érintett szervezet:
a) meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból lehető legkorlátozottabb módon – a szükséges minimum elv alapján – az elektronikus információs rendszerben használt információ technológiai termékekre a kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;
b) megvalósítja a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
c) a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;
d) figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett belső szabályzataival és eljárásaival összhangban.

KK. 6. 1. Automatikus támogatás
Automatikus mechanizmusokat kell alkalmazni a konfigurációs beállítások központi kezelésére, alkalmazására és ellenőrzésére.

KK 6. 2. Reagálás jogosulatlan változásokra
A szervezet által meghatározott intézkedéseket kell bevezetni a szervezet által meghatározott konfigurációs beállítások jogosulatlan változtatásainak észlelése esetén.

KK 7. Legszűkebb funkcionalitás
Az érintett szervezet:
a) az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;
b) meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok és/vagy szolgáltatások, szoftverek használatát.

KK 7. 1. Rendszeres felülvizsgálat

a) meghatározott gyakorisággal át kell vizsgálni az elektronikus információs rendszert, meg kell határozni és ki kell zárni, illetve le kell tiltani a szükségtelen és/vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat;
b) a szervezet által a szoftver használatra meghatározott szabályzatoknak és/vagy a szoftver használatára vonatkozó feltételeknek és kikötéseknek megfelelően az elektronikus információs rendszer megakadályozza a tiltott programok futtatását.

KK 7. 2. Nem futtatható szoftverek
Meg kell határozni, rendszeresen felül kell vizsgálni és frissíteni kell az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját és meg kell tiltani ezek futtatását;

KK 7. 3. Futtatható szoftverek
Meg kell határozni, rendszeresen felül kell vizsgálni és frissíteni kell az elektronikus információs rendszerben jogosultan futtatható (engedélyezett, úgynevezett fehérlistás) szoftverek listáját, és engedélyezni kell ezek futtatását, ettől eltérő szoftver futtatását egyedi engedélyhez kell kötni.

KK 8. Elektronikus információs rendszer elem leltár
Az érintett szervezet:
a) leltárt készít az elektronikus információs rendszer elemeiről;
b) meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszer elem leltárt.
Elvárás:
1. a leltár pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
2. az elektronikus információs rendszer hatókörébe eső valamennyi hardver és szoftver elemet tartalmazza,
3. legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

KK 8. 1. Frissítés
Történjen meg az elektronikus információs rendszer elem leltár frissítés az elemek telepítésének, eltávolításának, illetve frissítésének időpontjában.

KK 8. 2. Jogosulatlan elemek automatikus észlelése
a) automatizált mechanizmusok biztosítsák, hogy a szervezet által meghatározott gyakorisággal a jogosulatlan hardver, szoftver és firmware elemek észlelése megtörténjen;
b) a jogosulatlan elemek észlelése esetén le kell tiltani az ilyen elemek általi hálózati hozzáférését; el kell őket különíteni, és értesíteni kell az illetékes személyeket.

KK 8. 3. Duplikálás kivédése
Ellenőrizni kell, hogy az elektronikus információs rendszer hatókörén belül egyetlen elem sincs duplikálva más elektronikus információs rendszerek leltárában.

KK 8. 4. Automatikus támogatás

Automatikus mechanizmusokat kell alkalmazni az elektronikus információs rendszer elem leltár naprakész, teljes, pontos, és állandóan rendelkezésre álló kezelésének támogatására.

KK 8. 5. Naplózás
Az elektronikus információs rendszer elem leltárhoz csatolni kell az egyes elemek adminisztrálásáért felelős személyek nevét, pozícióját vagy szerepkörét.

KK 9. Konfigurációkezelési terv
Az érintett szervezet kialakít, dokumentál és végrehajt egy az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely:
a) figyelembe veszi a szerepköröket, felelősségeket és konfigurációkezelési folyamatokat és eljárásokat;
b) bevezet egy folyamatot a konfiguráció elemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfiguráció elemek konfigurációjának kezelésére;
c) meghatározza az elektronikus információs rendszer konfiguráció elemeit, és a konfiguráció elemeket a konfigurációkezelés alá helyezi;
d) védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

KK 10. A szoftver használat korlátozásai
Az érintett szervezet:
a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, illetve más jogszabályoknak;
b) a másolatok és szétosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftvereknek és a kapcsolódó dokumentációknak a használatát;
c) ellenőrzi és dokumentálja az azonos szintek közötti állomány megosztási technológiát, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

KK 11. A felhasználó által telepített szoftverek
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítését;
b) érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint;
c) meghatározott gyakorisággal ellenőrzi, és mindenkor érvényre juttatja a szabályok betartását.

ÜZLETMENET (ÜGYMENET) FOLYTONOSSÁG TERVEZÉSE, (ÜF)

ÜF 1 Üzletmenet folytonosságra vonatkozó eljárásrend
Az érintett szervezet:

a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező üzletmenet folytonosságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) az üzletmenet folytonossági tervben, vagy más szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti az üzletmenet folytonosságra vonatkozó eljárás rendet.

ÜF 2 Üzletmenet folytonossági terv informatikai erőforrás kiesésekre
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül érintett szervezet által kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel és/vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet folytonossági tervet;
b) összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;
c) meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet folytonossági tervét;
d) az elektronikus információs rendszer vagy a működtetési környezet változásainak, illetve az üzletmenet folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet folytonossági tervet;
e) tájékoztatja az üzletmenet folytonossági terv változásairól az a) pont szerintieket;
f) gondoskodik arról, hogy az üzletmenet folytonossági terv jogosulatlanok számára ne legyen megismerhető, illetve módosítható.
Elvárás:
1. meg kell határozni az alap feladatokat (biztosítandó szolgáltatásokat) és alap funkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket,
2. rendelkezni kell a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről,
3. ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket,
4. fenn kell tartani a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is (ez lehet egy külön katasztrófa elhárítási tervben is),
5. ki kell dolgozni a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

ÜF 2. 1. Egyeztetés
Az üzletmenet folytonossági tervet egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel.

ÜF 2. 2. Alap funkciók újraindítása

Meg kell határozni az alap funkciók újrakezdésének időpontját az üzletmenet folytonossági terv aktiválását követőn.

ÜF 2. 3. Kritikus rendszerelemek meghatározása
Meg kell határozni az elektronikus információs rendszer alap funkcióit támogató kritikus rendszer elemeket.

ÜF 2. 4. Kapacitástervezés
Meg kell tervezni a folyamatos működéshez szükséges információ feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást;

ÜF 2. 5. Összes funkció újraindítása
Meg kell határozni az összes funkció újrakezdésének időpontját az üzletmenet folytonossági terv aktiválását követően

ÜF 2. 6. Alap feladatok és funkciók folyamatossága
Az alap feladatok és funkciók folyamatosságát úgy kell megtervezni, hogy azok üzemelési folyamatosságában csak csekély vagy egyáltalán semmilyen veszteség ne álljon elő, és fent tudja tartani ezt a folyamatosságot az elektronikus információs rendszer elsődleges feldolgozó és/vagy tárolási helyszínén történő teljes helyreállításáig.

ÜF 3. A folyamatos működésre felkészítő képzés
Az érintett szervezet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, betöltött szerepkörüknek és felelősségüknek megfelelően:
a) szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;
b) meghatározott gyakorisággal, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

ÜF 3. 1. Szimuláció
A folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.

ÜF 4 Az üzletmenet folytonossági terv tesztelése
Az érintett szervezet:
a) meghatározott gyakorisággal és meghatározott tesztekkel teszteli az elektronikus információs rendszerre vonatkozó üzletmenet folytonossági tervet a terv hatékonyságának és a szervezet felkészültségének a felmérése céljából;
b) értékeli az üzletmenet folytonossági terv tesztelési eredményeit;
c) az értékelés alapján szükség esetén javítja a tervet, és a javításokkal kapcsolatban értékeli az üzletmenet folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el.

ÜF 4. 1. Koordináció
Az üzletmenet folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell.

ÜF 4. 2. Tartalék feldolgozási helyszín
Az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy a szervezet megismerje az adottságokat és az elérhető erőforrásokat és értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

ÜF 5. Biztonsági tárolási helyszín
Az érintett szervezet:
Kijelöl egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja;

ÜF 5. 1. Elkülönítés
A biztonsági tárolási helyszínnek el kell különülni az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

ÜF 5. 2. Elérhetőség
A biztonsági tárolási helyszínhez történő hozzáférés érdekében egy egész körzetre kiterjedő rombolás vagy katasztrófa esetére is eljárásokat kell kidolgozni.

ÜF 5. 3. Helyreállítás
A biztonsági tárolási helyszínt úgy kell kialakítani, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

ÜF 6. Tartalék feldolgozási helyszín
Az érintett szervezet:
a) kijelöl egy tartalék feldolgozási helyszínt, úgy, hogy amennyiben az elsődleges feldolgozási képesség nem áll rendelkezésére, elektronikus információs rendszere kritikus, vagy meghatározott műveleteket elvégzéséhez szükséges funkciókkal, meghatározott időn – összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal – belül a tartalék helyszínen újra kezdhesse;
b) biztosítja, hogy a szállításhoz és a működés újrakezdéséhez szükséges eszközök és ellátások a tartalék feldolgozási helyszínen rendelkezésre állnak, vagy azok szükség esetén meghatározott időn belül rendelkezésre fognak állni;
c) biztosítja, hogy a tartalék feldolgozási helyszín informatika biztonsági intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.

ÜF 6. 1. Elkülönítés

Olyan tartalék feldolgozási helyszínt kell meghatározni, amely elkülönül az elsődleges feldolgozás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

ÜF 6. 2. Elérhetőség
Az alternatív feldolgozási helyszínhez történő hozzáférésé érdekében egy egész körzetre kiterjedő rombolás vagy katasztrófa esetére is eljárásokat kell kidolgozni.

ÜF 6. 3. Szolgáltatások priorálása
A tartalék feldolgozási helyszínre vonatkozóan olyan megállapodásokat kell kötni, intézkedéseket kell bevezetni, amelyek a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban álló szolgáltatás-prioritási rendelkezéseket tartalmaznak.

ÜF 6. 4. Előkészület a működés megindítására
Az érintett szervezet úgy készíti fel a tartalék feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alap funkciók működésének támogatására.

ÜF-7 Infokommunikációs szolgáltatások
A Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével az érintett szervezet tartalék infokommunikációs szolgáltatásokat létesít, illetve erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alap funkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését amennyiben az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

ÜF 7. 1. Szolgáltatások prioritása
Amennyiben az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

ÜF 7. 2. Közös hibalehetőségek kizárása
Olyan tartalék infokommunikációs szolgáltatásokat kell igénybe venni, melyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).

ÜF-8 Az elektronikus információs rendszer mentései
Az érintett szervezet:
a) meghatározott gyakorisággal mentést végez (elmenti) az elektronikus információs rendszerben tárolt felhasználó-szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

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

ÜF 8. 1. Megbízhatósági és sértetlenségi teszt
Meghatározott gyakorisággal tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.

ÜF 8. 2. Helyreállítási teszt
az üzletmenet folytonossági terv tesztelésének részeként egy kiválasztott mintát kell használni a biztonsági másolat információkból az elektronikus információs rendszer kiválasztott funkcióinak helyreállításánál.

ÜF 8. 3. Kritikus információk elkülönítése
Az elektronikus információs rendszer szervezet által meghatározott kritikus szoftverei és egyéb biztonsággal kapcsolatos információk biztonsági másolatait egy elkülönített berendezésen vagy egy minősítéssel rendelkező tűzbiztos tárolóban kell tárolni.

ÜF 8. 4. Alternatív tárolási helyszín
Az elektronikus információs rendszer biztonsági másolat információit a biztonsági tárolási helyszínen (ÜF 5.) kell tárolni.

ÜF 9. Az elektronikus információs rendszer helyreállítása és újraindítása
Az érintett szervezet gondoskodik az elektronikus információs rendszer ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

ÜF 9. 1. Tranzakciók helyreállítása
Tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítást kell végre hajtani.

ÜF 9. 2. Helyreállítási idő
Biztosítani kell azt a lehetőséget, hogy az elektronikus információs rendszer elemeket előre definiált helyreállítási idő alatt helyre lehessen állítani egy olyan konfiguráció-ellenőrzött és sértetlenség-védett információból, ami az elem ismert működési állapotát reprezentálja.

KARBANTARTÁS (KA)

KA-1 Rendszer karbantartási eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező rendszer karbantartási kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a fizikai védelmi eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.

KA-2 Rendszeres karbantartás
Az érintett szervezet:
a) karbantartásokat és javításokat ütemez, hajt végre és dokumentál az elektronikus információs rendszer elemeken és felülvizsgálja az ezekről készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és/vagy a szervezeti követelményeknek megfelelően;
b) jóváhagyja és figyeli az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;
c) megköveteli, hogy az ezért felelős személyek hagyják jóvá az elektronikus információs rendszer vagy a rendszer elemek elvitelét a szervezeti létesítményből más helyszínre;
d) elszállítás előtt minden adatot és információt töröl (mentés után) a berendezésről;
e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e; és biztonsági ellenőrzésnek veti alá azokat;
f) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

KA 2. 1. Automatikus támogatás
Az érintett szervezet
a) automatizált mechanizmusokat alkalmaz a karbantartások és javítások ütemezésére, lefolytatására és dokumentálására;
b) naprakész, pontos és teljes nyilvántartást készít minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási akcióról.

KA 3. Karbantartási eszközök
Az érintett szervezet jóváhagyja, nyilvántartja és ellenőrzi az elektronikus információs rendszer karbantartási eszközeit.

KA 3. 1. Ellenőrzés
Ellenőrizni kell a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.

KA 3. 2. Adathordozó ellenőrzés

Ellenőrizni kell a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

KA 3. 3.
Az érintett szervezet:
Meggátolja, hogy információt tartalmazó karbantartási eszközt jogosulatlanul elszállítsanak, azzal, hogy:

1) ellenőrzi, hogy az eszköz nem tartalmaz-e információt, vagy;
2) törli vagy megsemmisíti az eszközt, vagy;
3) az eszközt a létesítményen belül őrzi;
4) valamint az ezért felelős személyekkel engedélyezteti az eszköz elszállítását a létesítményből.

KA 4. Távoli karbantartás
Az érintett szervezet:
a) jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;
b) akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal és dokumentálva van az elektronikus információs rendszerbiztonsági tervben;
c) hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;
d) nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;
e) lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

KA 4. 1. Dokumentálás
Az érintett szervezet az elektronikus információs rendszer rendszerbiztonsági tervében dokumentálja a távoli karbantartási és diagnosztikai kapcsolatok létrehozására és használatára vonatkozó szabályokat és eljárásokat.

KA 4. 2. Összehasonlítható biztonság
a) meg kell követelni, hogy a távoli karbantartási és diagnosztikai szervizelések olyan elektronikus információs rendszerből legyenek végrehajtva, amelyben a megvalósított biztonsági képességek azonos szintűek a szervizelt rendszeren megvalósított biztonsági képességekkel; vagy
b) el kell távolítani a szervizelendő elemet az elektronikus információs rendszerből, és a távoli karbantartási és diagnosztikai szervizelést megelőzően minden információt törölni kell az az érintett rendszerelemről;
c) a szervizelés végrehajtását követően át kell vizsgálni az elemet (a lehetséges kártékony szoftverek miatt), mielőtt visszakapcsoljak az elektronikus információs rendszerhez.

KA 5. Karbantartók
Az érintett szervezet:

a) kialakít egy folyamatot a karbantartók engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
b) biztosítja, hogy az elektronikus információs rendszeren karbantartást végzőktől megköveteljék a hozzáférési jogosultság igazolását;
c) kinevez a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeket arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

KA 5. 1. Karbantartás fokozott biztonsági intézkedésekkel
a) megfelelő biztonsági engedéllyel nem rendelkező, vagy nem magyar állampolgárú karbantartó személyek alkalmazása során:
1. az ilyen karbantartó személyeket megfelelő hozzáférési jogosultságú, műszakilag képzett belső személyeknek kell kísérnie és felügyelnie az elektronikus információs rendszeren végzett karbantartási és diagnosztikai tevékenységek során,
2. a karbantartási és diagnosztikai tevékenységek megkezdése előtt az elektronikus információs rendszer minden fellelhető információtároló elemét törölni kell, és a nem törölhető adathordozót el kell távolítani vagy fizikailag le kell választani a rendszertől;
b) alternatív biztonsági védelmeket kell kialakítani, ha egy elektronikus információs rendszer elemet nem lehet törölni, eltávolítani vagy a rendszertől leválasztani.

KA 6. Időben történő javítás
Az érintett szervezet karbantartási támogatást és/vagy tartalék alkatrészeket szerez be a meghatározott elektronikus információs rendszer elemekhez.

ADATHORDOZÓK VÉDELME (AV)

AV 1. Adathordozók védelmére vonatkozó eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az adathordozók védelmére vonatkozó eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező adathordozók védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) az adathordozók védelmére vonatkozó eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti az adathordozók védelmére vonatkozó eljárásrendet.

AV 2. Hozzáférés az adathordozókhoz
Az érintett szervezet a meghatározott digitális és/vagy nem-digitális adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza, illetve korlátozza.

AV 3. Adathordozók címkézése

Az érintett szervezet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket (ha van ilyen);

AV 4. Adathordozók tárolása
Az érintett szervezet:
a) fizikailag ellenőrzi és biztonságosan tárolja az adathordozókat, az arra engedélyezett, vagy kijelölt helyen;
b) védi az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

AV 5. Adathordozók szállítása
Az érintett szervezet:
a) meghatározott biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;
b) biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;
c) dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;
d) korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

> AV 5. 1. Kriptográfiai védelem
> Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán.

AV 6 Adathordozók törlése
Az érintett szervezet:
a) meghatározott törlési technikákkal és eljárásokkal törli elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt;
b) a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

> AV 6. 1. Ellenőrzés
> Az érintett szervezet felülvizsgálja, jóváhagyja, nyomon követi, dokumentálja és ellenőrzi az adathordozók törlésével és megsemmisítésével kapcsolatos tevékenységeket.
>
> AV 6. 2. Tesztelés
> A törlésre alkalmazott eszközöket és eljárásokat meghatározott gyakorisággal tesztelni kell.
>
> AV 6. 3. Törlés megsemmisítés nélkül

Nem-romboló törlési technikák alkalmazhatók a meghatározott hordozható tároló eszközökre, mielőtt ilyen eszközöket az elektronikus információs rendszerhez csatolnak.

AV 7 Adathordozók használata
Az érintett szervezet engedélyezi, korlátozza; vagy tiltja egyes adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszer elemeken működő biztonsági intézkedések használatával.

AV 7. 1. Ismeretlen tulajdonos
Az érintett szervezet megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

AZONOSÍTÁS ÉS HITELESÍTÉS (AH)

AH-1 Azonosítási és hitelesítési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező azonosítási és hitelesítési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) az azonosítási és hitelesítésre vonatkozó eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti az azonosítási és hitelesítésre vonatkozó eljárásrendet.

AH 2. Azonosítás és hitelesítés (szervezeten belüli felhasználók)
Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett szervezeten belüli felhasználókat, illetve a felhasználók által végzett tevékenységet.

AH 2. 1. Hálózati hozzáférés privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött (privilegizált) felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

AH 2. 2. Hálózati hozzáférés nem privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

AH 2. 3. Helyi hozzáférés privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

AH 2. 4. Visszajátszás-védelem
Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

AH 2. 5. Távoli hozzáférés – külön eszköz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

AH 2. 6. Helyi hozzáférés nem privilegizált fiókokhoz
Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

AH 2. 7. Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz
Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

AH-3 Eszközök azonosítása és hitelesítése
Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket és/vagy eszköz típusokat mielőtt helyi, távoli, hálózati kapcsolatot létesítene velük.

AH 4. Azonosító kezelés
Az érintett szervezet:
a) egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti;
b) hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;
c) meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását;
d) meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.

AH 5. A hitelesítésre szolgáló eszközök kezelése
Az érintett szervezet az alábbi módon kezeli az elektronikus információs rendszer hitelesítésre szolgáló eszközeit:
a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;
b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;
c) biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett/kompromittálódott vagy sérült eszközöket;
e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;

g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja/frissíti a hitelesítésre szolgáló eszközöket;
h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;
i) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

AH 5 1. Jelszó alapú hitelesítés
Az érintett szervezet:
a) a jelszóra minimális bonyolultságot juttat érvényre a következő elvárásokkal: kis és nagy betűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek minimális száma;
b) meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;
c) a jelszavakat csak feltétlen szükséges esetben és csak titkosított formában tárolja és továbbítja;
d) a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, illetve a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

AH 5 2. Hardver token alapú hitelesítés
Az elektronikus információs rendszer hardver token alapú hitelesítés esetén olyan mechanizmusokat alkalmaz, mely megfelel az érintett szervezet által meghatározott minőségi követelményeknek.

AH-5 (3) PKI alapú hitelesítés
Az érintett szervezet az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:
a) ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;
b) kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;
c) összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal;
d) megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

AH-5 (4) Személyes vagy megbízható harmadik fél általi regisztráció
Az érintett szervezet meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet] folytat le az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

AH 6. A hitelesítésre szolgáló eszköz visszacsatolása

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

AH 7. Hitelesítés kriptográfiai modul esetén
Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

AH 8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)
Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett szervezeten kívüli felhasználókat, illetve a tevékenységüket.

AH 8. 1.Hitelesítés szolgáltatók tanúsítványának elfogadása
Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

HOZZÁFÉRÉS ELLENŐRZÉSE (HE)

HE 1. Hozzáférés ellenőrzési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező a hozzáférés ellenőrzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a hozzáférés védelmére vonatkozó eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti az a hozzáférések védelmére vonatkozó eljárásrendet.

HE 2. Felhasználói fiókok kezelése
Az érintett szervezet:
a) meghatározza és kiválasztja az elektronikus információs rendszer felhasználói fiókokat, és ennek típusait;
b) kijelöli az elektronikus információs rendszer felhasználói fiókok fiókkezelőit;
c) kialakítja a csoport és szerepkör tagsági feltételeket;
d) meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;
e) létrehozza, engedélyezi, módosítja, letiltja és eltávolítja az elektronikus információs rendszer felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;
f) ellenőrzi az elektronikus információs rendszer felhasználói fiókok használatát;
g) értesíti a fiókkezelőket:
1. ha a felhasználói fiókokra már nincsen szükség,

2. ha a felhasználók kiléptek vagy áthelyezésre kerültek,
3. ha az elektronikus információs rendszer használata vagy az ehhez szükséges legkisebb tudás mértéke változik;

h) feljogosít az elektronikus információs rendszerhez való hozzáférésre a:
1. érvényes hozzáférési engedély,
2. tervezett rendszerhasználat,
3. az alapfeladatok és funkcióik
alapján;

i) meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat a fiókkezelési követelményekkel való összhangot;

j) kialakít egy folyamatot a megosztott/csoport felhasználói fiókokhoz tartozó hitelesítő eszközök/adatok újra kibocsátására (ha ilyent alkalmaznak), a csoport tagjainak változása esetére.

HE 2. 1. Automatikus kezelés
Az elektronikus információs rendszer alkalmazzon automatizált mechanizmusokat az elektronikus információs rendszer fiókjainak kezeléséhez.

HE 2. 2. Ideiglenes fiókok eltávolítása
Meghatározott időtartam letelte után elektronikus információs rendszer automatikusan távolítsa el, vagy tiltsa le az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat, vagy egyes kijelölt felhasználói fiók típusokat.

HE 2. 3. Inaktív fiókok letiltása
Az elektronikus információs rendszer automatikusan tiltsa az inaktív fiókokat meghatározott időtartam letelte után.

HE 2. 4. Automatikus naplózás
Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesítse ezekről a meghatározott személyeket vagy szerepköröket.

HE 2. 5. Kiléptetés
Meghatározott időtartamú várható inaktivitás, vagy egyéb előre meghatározott esetekben meg kell követelni a felhasználó kiléptetését.

HE 2. 6. Szokatlan használat
Figyelni kell az elektronikus információs rendszer fiókjait a szervezet által meghatározott szokatlan használat szempontjából, és meghatározott személyeknek vagy szerepköröknek jelenteni kell azt.

HE 2. 7. Letiltás
A lehető legrövidebb időn belül le kell tiltani a jelentős kockázatú felhasználók fiókjait.

HE 3. Hozzáférés ellenőrzés érvényre juttatása
Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényre juttatja a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

HE 4. Információ áramlás ellenőrzés érvényre juttatása
Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényre juttatja a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információ áramlás ellenőrzéséhez az érintett szervezet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

HE 5. A felelősségek szétválasztása
Az érintett szervezet:
a) szétválasztja az egyéni felelősségeket;
b) dokumentálja az egyéni felelősségek szétválasztását;
c) meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztásának támogatására.

HE 6. Legkisebb jogosultság elve
Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazva a felhasználók (illetve a felhasználók tevékenysége) számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

HE 6. 1. Jogosult hozzáférés a biztonsági funkciókhoz
Hozzáférési jogosultságokat ad a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

HE 6. 2. Nem privilegizált hozzáférés a biztonsági funkciókhoz
Megköveteli, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához ne a privilegizált fiókjukat vagy szerepkörüket használják.

HE 6. 3. Privilegizált fiókok
Az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

HE 6. 4. Privilegizált funkciók használatának naplózása
Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.

HE 6. 5. Privilegizált funkciók tiltása nem privilegizált felhasználóknak
Az elektronikus információs rendszer akadályozza meg, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását.

HE 6. 6. Hálózati hozzáférés a privilegizált parancsokhoz
A meghatározott privilegizált parancsok hálózaton keresztüli elérése csak meghatározott kényszerítő üzemeltetési szükség esetén engedélyezhető, és az ilyen hozzáférések indoklását dokumentálni kell a rendszerbiztonsági tervben. Privilegizált parancsok alapesetben csak meghatározott munkaállomásokról, terminálokról, szegmensekről és IP címekről adhatóak ki, mely munkaállomások/terminálok helyiségei fizikai hozzáférés szempontjából normáltól eltérő szintű besorolást kapnak.

HE 7. Sikertelen bejelentkezési kísérletek
Az elektronikus információs rendszer:
a) az érintett szervezet által meghatározott számként megadott korlátot juttat érvényre egy felhasználó egymást követő bejelentkezési kísérleteire, amelyek meghatározott időtartamon belül történtek;
b) amennyiben a sikertelen kísérletek a maximális számot túllépik, az információs rendszer automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, illetve meghatározott módon késlelteti a következő bejelentkezési kísérletet.

HE 8. A rendszerhasználat jelzése
Az érintett szervezet az elektronikus információs rendszer felhasználásával:
a) az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:
1. a felhasználó az érintett szervezet elektronikus információs rendszerét használja,
2. a rendszer használatot figyelhetik, rögzíthetik, illetve naplózhatják,
3. a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár,
4. a rendszer használata egyben a felhasználó beleegyezését is jelenti előbbiekbe;
b) a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez;
c) nyilvánosan elérhető rendszerek esetén:
1. kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít,
2. amennyiben felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak,
3. leírást biztosít a rendszer engedélyezett felhasználásáról.

HE 9. Egyidejű munkaszakasz kezelés
Az érintett szerv az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok és/vagy fiók típusok számára külön-külön.

HE 10 A munkaszakasz zárolása

Az érintett szervezet:
a) meghatározott időtartam inaktivitás után, vagy a felhasználó erre irányuló kérése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;
b) megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

HE 10 1. Képernyőtakarás
A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel) kell eltakarni.

HE 11. A munkaszakasz lezárása
Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

HE 12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek
Az érintett szervezet:
a) kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani;
b) dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.

HE 13. Távoli hozzáférés
Az érintett szervezet:
a) kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási/kapcsolódási követelményeket és a megvalósítási útmutatókat;
b) engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

HE 13. 1. Ellenőrzés
Az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket.

HE 13. 2. Titkosítás
Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére.

HE 13. 3. Hozzáférés ellenőrzési pontok
Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben.

HE 13. 4. Privilegizált parancsok elérése
Az érintett szervezet:

a) privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez;
b) dokumentálja és indokolja az a) pont szerinti hozzáféréseket a rendszerbiztonsági tervben.

HE 14. Vezeték nélküli hozzáférés
Az érintett szervezet:
a) belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
b) engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

HE 14. 1. Hitelesítés és titkosítás
Az elektronikus információs rendszerben titkosítással és a felhasználók, vagy eszközök hitelesítésével védi a vezeték nélküli hozzáférést.

HE 14. 2. Felhasználó konfigurálás tiltása
Azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását.

HE 14. 3. Antennák
Olyan karakterisztikájú és teljesítmény szintű antennákat és árnyékolási megoldásokat üzemeltet, vagy egyéb technikákat alkalmaz, amelyekkel csökkenti a szervezet fizikai védelmi határain kívül a jelek észlelésének a valószínűségét.

HE 15. Mobil eszközök hozzáférés ellenőrzése
Az érintett szervezet:
a) belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;
b) engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

HE 15. 1. Titkosítás
Teljes eszköztitkosítást, vagy tároló-alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

HE 16. Külső elektronikus információs rendszerek használata
Az érintett szervezet
a) meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó
egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;

b) külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó eldolgozni, tárolni vagy továbbítani a szervezet által ellenőrzött információkat.

HE 16. 1. Korlátozott használat
A szervezet csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, illetve a által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

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

HE 16. 2. Hordozható adattároló eszközök
Korlátozza, vagy megtiltja az ellenőrzött hordozható tároló eszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező személyek számára.

HE 17. Információ megosztás
Az érintett szervezet:
a) elősegíti az információ megosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információ megosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;
b) automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információ megosztási/együttműködési döntések meghozatalában.

HE 18. Nyilvánosan elérhető tartalom
Az érintett szervezet:
a) kijelöli azokat a személyeket, akik jogosultak a szervezettel kapcsolatos bármely információ közzétételére nyilvánosan hozzáférhető elektronikus információs rendszeren;
b) az a) pont szerinti személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;
c) közzététel előtt átvizsgálja a javasolt tartalmat;
d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.

RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉG (RS)

Jelen fejezet egyes rendelkezéseit egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert az érintett szerv üzemelteti. Üzemeltetési szolgáltatási szerződés esetén a szerződéses kötelemként kell érvényesíteni a jelen fejezetben foglaltak, és azokat a szolgáltatónak kell biztosítania.

RS 1. Rendszer és információ sértetlenségre vonatkozó eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti a rendszer és információ sértetlenségre vonatkozó eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező a rendszer és információ sértetlenségre vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a rendszer és információ sértetlenségre vonatkozó eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti az a hozzáférések védelmére vonatkozó eljárásrendet.

RS 2. Hibajavítás
Az érintett szervezet:
a) azonosítja, belső eljárásrendje alapján jelenti és kijavítja, vagy kijavíttatja az elektronikus információs rendszer hibáit;
b) telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;
c) a biztonságkritikus szoftvereket frissítésük kiadását követő meghatározott időtartamon] belül telepíti, vagy telepíttetni;
d) beépíti a hibajavítást a konfigurációkezelési folyamatba.

RS 2. 1. Automatizált hibajavítási állapot
Automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemeinek hibajavítási állapotának meghatározására.

RS 2. 2. Központi kezelés
Központilag kezeli a hibajavítás folyamatát.

RS 3. Kártékony kódok elleni védelem
Az érintett szervezet:
a) az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;
b) frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfiguráció kezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kód irtó rendszeréhez frissítések jelennek meg;
c) konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:
1. rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, és/vagy a hálózati belépési/kilépési pontokon, a

biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

2. a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt; és riassza az adminisztrátort;

d) ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

RS. 3. 1. Központi kezelés

Központilag kezeli és a kártékony kódok elleni védelmi mechanizmusokat.

RS 3. 2. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

RS 4. Az elektronikus információs rendszer felügyelete

Az érintett szervezet:

a) felügyeli az elektronikus információs rendszert, hogy észlelje a támadásokat és a lehetséges támadások jeleit a meghatározott figyelési céloknak megfelelően, valamint feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;

b) azonosítja az elektronikus információs rendszer jogosulatlan használatát meghatározott technikák és módszerek segítségével;

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

d) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

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

f) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

RS 4. 1. Automatizálás

Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.

RS 4. 2. Felügyelet

Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel.

RS 4. 3. Riasztás

Az elektronikus információs rendszer riassza a szervezet illetékes személyeit, illetve csoportjait, amikor veszélyeztetésnek vagy potenciális veszélyeztetésnek előállnak az előre meghatározott jelei:

RS 5. Biztonsági riasztások és tájékoztatások
Az érintett szervezet:
a) folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
b) folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
c) szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;
d) eljuttatja ezeket az illetékes személyekhez;
e) megfelelő válaszlépéseket tesz.

RS 5. 1. Automatikus riasztások
Mechanizmusokat kell kialakítani a biztonsági riasztások és figyelmeztetések szervezeten belüli elérhetőségének biztosítására.

RS 6. A biztonsági funkcionalitás ellenőrzése
Az elektronikus információs rendszer:
a) ellenőrzi a beállított biztonsági funkciókat az ellenőrzésre jogosult felhasználó utasítására, vagy időszakosan;
b) értesítést küld az érintett szervezet által meghatározott személyeknek vagy szerepköröknek, ha az ellenőrzés hibát tár fel;
c) rendellenesség észlelése esetén leállítja a rendszert, és/vagy újraindítja a rendszert, és/vagy egyéb ellenintézkedést valósít meg.

RS 7. Szoftver és információ sértetlenség
Az érintett szervezet sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.

RS 7. 1. Sértetlenség ellenőrzés
Az elektronikus információs rendszer sértetlenség ellenőrzést hajt végre a meghatározott szoftverekre és információkra, a rendszer újraindításakor, vagy biztonsági esemény bekövetkezését követően, illetve meghatározott gyakorisággal.

RS 7. 2. Észlelés és reagálás
Az érintett szervezet beépíti az elektronikus információs rendszer jogosulatlan változtatásainak észlelését a biztonsági eseményekre reagáló eljárásaiba.

RS 7. 3. Automatikus értesítés
Automatizált eszközöket alkalmaz a meghatározott személyek vagy szerepkörök értesítésére, ha a sértetlenség ellenőrzés rendellenességet tár fel.

RS 7. 4. Automatikus reagálás
Az elektronikus információs rendszer automatikusan leállítja, vagy újraindítja a rendszert, vagy egyéb intézkedést valósít meg, ha a sértetlenség ellenőrzés rendellenességet tár fel.

RS 7. 5. Végrehajtható kód
Megtiltja az olyan bináris vagy gépi kód használatát, mely nem ellenőrzött forrásból származik, vagy melynek forráskódjával nem rendelkezik.

RS 8. Levélszemét elleni védelem
Az érintett szervezet:
a) levélszemét (kéretlen üzenetek) elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében;
b) új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.

RS 8. 1. Központi kezelés
Központi beállításokkal irányítja a levélszemét elleni védelmet.

RS 8. 2. Frissítés
Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival

RS 9. Bemeneti információ ellenőrzés
Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.

RS 10. Hibakezelés
Az elektronikus információs rendszer:
a) hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak;
b) a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.

RS 11. A kimeneti információ kezelése és megőrzése
Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

RS 12. Memória védelem
Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától.

NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG (NA)

NA 1. Naplózási eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül szabályzóiban meghatározott személyek vagy szerepkörök számára

kihirdeti a naplózási eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a naplózásra és elszámoltathatóságra vonatkozó eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti az a hozzáférések védelmére vonatkozó eljárásrendet.

NA 2. Naplózható események
Az érintett szervezet:
a) meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;
b) egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;
c) megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

NA 2. 1. Felülvizsgálat
Meghatározott gyakorisággal felülvizsgálja és aktualizálja a naplózandó eseményeket.

NA 3. Naplóbejegyzések tartalma
Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

NA 3. 1. Kiegészítő információk
A naplóbejegyzésekben további az érintett szervezet által meghatározott kiegészítő, részletesebb információkat is rögzít.

NA 3. 2. Központi kezelés
Biztosítsa a meghatározott rendszer elemek által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását.

NA 4. Napló tárkapacitás
Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít.

NA 5. Naplózási hiba kezelése
Az elektronikus információs rendszer
a) naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;
b) elvégzi a meghatározott végrehajtandó tevékenységek, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

NA 5. 1. Naplózási tárhely ellenőrzés

Figyelmezteti a meghatározott személyeket, szerepköröket és/vagy helyszíneket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét.

NA 5. 2. Valósidejű riasztás
Riasztást küld, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik.

NA 6. Napló vizsgálat és jelentéskészítés
Az érintett szervezet:
a) rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából;
b) jelenti ezeket a meghatározott személyeknek, vagy szerepköröknek.

NA 6. 1. Folyamatba illesztés
Automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a gyanús tevékenységekre reagál és kivizsgálja azokat.

NA 6. 2. Összegzés
Megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, hogy a teljes szervezetre kiterjedő helyzetfelmérést nyerjen.

NA 6. 3. Felügyeleti képességek integrálása
Egyesíti a naplóbejegyzések vizsgálatát a sebezhetőség ellenőrzési információk, a teljesítmény adatok, az elektronikus információs rendszer felügyeletéből származó információk, vagy egyéb forrásokból begyűjtött adatok/információk vizsgálatával, hogy tovább erősítse a nem megfelelő vagy szokatlan tevékenységek megállapításának képességét.

NA 6. 4. Összekapcsolás a fizikai hozzáférési információkkal
Összefüggésbe hozza a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert információkkal, hogy tovább erősítse a gyanús, nem megfelelő, szokatlan vagy rosszindulatú tevékenységek megállapításának képességét.

NA 7. Naplócsökkentés és jelentéskészítés
Az elektronikus információs rendszer
a) biztosítson lehetőséget naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő napló áttekintési, vizsgálati és jelentés készítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;
b) nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

NA 7. 1. Automatikus feldolgozás
Biztosítsa, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.

NA 8. Időbélyegek
Az elektronikus információs rendszer
a) belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;
b) időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz (UTC) vagy a Greenwichi középidőhöz (GMT) rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak.

NA 8. 1. Szinkronizálás
Meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles időforrással, és szinkronizálja a belső rendszer órákat a hiteles külső időforrással, ha az időeltérés nagyobb, mint a meghatározott időtartam.

NA 9. A napló információk védelme
Az elektronikus információs rendszer megvédi a napló információt és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

NA 9. 1. Hozzáférés korlátozás
A napló funkciók kezelésére csak a privilegizált felhasználók szervezet által meghatározott része jogosult.

NA 9. 2. Fizikailag elkülönített mentés
A naplóbejegyzéseket meghatározott gyakorisággal elmenti egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszer elemre.

NA 9. 3. Kriptográfiai védelem
Kriptográfiai mechanizmusokat kell alkalmazni a napló információ és a naplózó eszköz sértetlenségének védelmére.

NA 10. Letagadhatatlanság
Az elektronikus információs rendszer védelmet kell biztosítania az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében alkalmazás letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.

NA 11. A naplóbejegyzések megőrzése
Az érintett szervezet a naplóbejegyzéseket, meghatározott, az adatmegőrzésre vonatkozó szabályzattal összhangban álló időtartamig megőrzi azért, hogy támogatást nyújtson a biztonsági események utólagos kivizsgálására, és hogy megfeleljen a jogszabályi és szervezeten belüli információ megőrzési követelményeknek.

NA 12. Naplógenerálás
Az elektronikus információs rendszer
a) biztosítja a naplóbejegyzés generálási lehetőségét az NA-2 a) bekezdése alatt meghatározott naplózható eseményekre;

b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek], hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;
c) naplóbejegyzéseket állít elő a NA 2. a) bekezdése szerinti eseményekre az NA-3-ban meghatározott tartalommal.

NA 12. 1. Rendszerszintű időalap napló
A naplóbejegyzéseiből rendszerszintű (logikai vagy fizikai) felülvizsgálati naplót állít össze, amely az (felülvizsgálati napló egyedi bejegyzéseinek időbélyegei közötti kapcsolat tekintetében meghatározott tűréshatáron túli) időviszonyokat is tartalmazza.

NA 12. 2. Változtatások
Biztosítja a lehetőséget a meghatározott személyeknek vagy szerepköröknek arra, hogy megváltoztassák az egyes rendszer elemekre végrehajtandó naplózást a kiválasztott esemény kritériumok alapján, meghatározott időtartamon belül.

RENDSZER ÉS KOMMUNIKÁCIÓ VÉDELEM (RV)

RV-1 Rendszer és kommunikáció védelmi eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül szabályzóiban meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer és kommunikáció védelmi eljárásrendet, mely szervezet informatikai biztonsági szabályzatának részét képező rendszer és kommunikáció védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a rendszer és kommunikáció védelmi eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer és kommunikáció védelmére vonatkozó eljárásrendet.

RV 2. Alkalmazás szétválasztás
Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.

RV 3. Biztonsági funkciók elkülönítése
Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

RV 4. Információ maradványok
Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan és véletlen információáramlást.

RV 5. Túlterhelés (Szolgáltatás megtagadás alapú támadás) elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

RV 6. A határok védelme
Az elektronikus információs rendszer
a) felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációkat;
b) a nyilvánosan hozzáférhető rendszer elemeket fizikailag és/vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;
c) csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

RV 6. 1. Hozzáférési pontok
Az érintett szervezet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.

RV 6. 2. Külső kommunikációs szolgáltatások
Az érintett szervezet
a) felügyelt interfészt valósít meg minden külső infokommunikációs szolgáltatáshoz;
b) minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;
c) védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;
d) dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alap feladattal és az igényelt kivétel időtartamával együtt;
e) meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alap feladat már nem indokol.

RV 6. 3. Alapeseti visszautasítás
Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat (vagyis minden tiltva, engedélyezés kivételes esetben).

RV 6. 4. Távoli készülékek megosztott csatorna használatának tiltása
A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.

RV 6. 5. Hitelesített proxy kiszolgálók
Az elektronikus információs rendszer hitelesített proxy kiszolgálók segítségével irányítja a belső kommunikációs forgalmat a felügyelt interfészeken a meghatározott külső hálózatokhoz].

RV 6. 6. Biztonsági hibaállapot
Az elektronikus információs rendszer hibaállapotba kerül a határvédelmi eszköz működési hibája esetén.

RV 6. 7. Rendszer elemek elkülönítése
Az érintett szervezet
Határvédelmi mechanizmusokat alkalmaz azoknak az elektronikus információs rendszer elemeknek az elkülönítésére, amelyek a meghatározott alap feladatokat és/vagy funkciókat támogatják.

RV 7. Az adatátvitel bizalmassága
Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát.

RV 7. 1. Kriptográfiai vagy egyéb védelem
Alkalmazzon kriptográfiai mechanizmusokat az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett.

RV 8. Az adatátvitel sértetlensége
Az elektronikus információs rendszer védje meg a továbbított információk sértetlenségét.

RV 8. 1. Kriptográfiai, vagy egyéb védelem
Alkalmazzon kriptográfiai mechanizmusokat az adatátvitel során az információk megváltozásának észlelésére, amennyiben az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

RV 9. A hálózati kapcsolat megszakítása
Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor meghatározott időtartamú inaktivitás után.

RV 10. Kriptográfiai kulcs előállítása és kezelése
Az érintett szervezet állítsa elő és kezelje az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

RV 10. 1. Rendelkezésre állás
Biztosítsa az információk rendelkezésre állását abban az esetben is, amikor a kriptográfiai kulcsok elérhetetlenné válik (elvesztés, sérülés, megsemmisülés).

RV 11. Kriptográfiai védelem
Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

RV 12. Együttműködésen alapuló számítástechnikai eszközök
Elvárás:
1. az elektronikus információs rendszer gátolja meg az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt;
2) közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

RV 13. Nyilvános kulcsú infrastruktúra tanúsítványok
Az érintett szervezet nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatótól.

RV 14. Mobil kód korlátozása
Az érintett szervezet:
a) meghatározza az elfogadható és a nem elfogadható mobil kódokat és mobil kód technológiákat;
b) használati korlátozásokat vezet be, illetve megvalósítási útmutatót bocsát ki az elfogadható mobil kódokra és mobil kód technológiákra;
c) engedélyezi, felügyeli és ellenőrzi a mobil kódok használatát az elektronikus információs rendszeren belül.

RV 15. Interneten keresztüli hangátvitel (VoIP)
Az érintett szervezet:
a) használati korlátozásokat vezet be, illetve megvalósítási útmutatót ad az interneten keresztüli hangátvitel (VoIP) technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat;
b) engedélyezi, felügyeli és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.

RV 16. Biztonságos név/cím feloldó szolgáltatások (hiteles forrás)
Elvárás:
1. az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít;
2. ha egy elosztott, hierarchikus névtér részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód és előd tartományok közötti bizalmi láncot.

RV 17. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)
Az elektronikus információs rendszer eredet hitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

RV 18. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén
Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

RV 19. Munkaszakasz hitelessége
Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét.

RV 20. Hibát követő ismert állapot
Meghatározott hibatípusokhoz tartozó hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerül, amely hiba esetén megőrzi a rendszer állapot információkat.

RV 21. A maradvány információ védelme
Az elektronikus információs rendszer védje az érintett szervezet által meghatározott maradvány információk bizalmasságát; sértetlenségét.

RV 22. A folyamatok elkülönítése
Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

REAGÁLÁS A BIZTONSÁGI ESEMÉNYEKRE (RE)

RE-1 Biztonsági eseménykezelési eljárásrend
Az érintett szervezet:
a) megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül szabályzóiban meghatározott személyek vagy szerepkörök számára kihirdeti a biztonsági eseménykezelési eljárásrendet, mely szervezet informatikai biztonsági szabályzatának (vagy egyéb belső szabályzat) részét képező elektronikus információbiztonsági esemény kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;
b) a biztonsági eseménykezelési eljárásrendben, vagy más belső szabályzóban meghatározott gyakorisággal felülvizsgálja és frissíti biztonsági eseménykezelésre vonatkozó eljárásrendet.

RE 2. Képzés a biztonsági események kezelésére
Az érintett szervezet
a) biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;
b) a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, illetve meghatározott gyakorisággal tartja.

RE 2. 1. Szimuláció
A biztonsági esemény kezelési képzésébe szimulált eseményeket foglaljon bele, hogy elősegítse a személyzet hatékony reagálását kritikus helyzetekben.

RE 2. 2. Automatizált képzési környezet
Alkalmazzon automatizált mechanizmusokat, hogy biztonsági esemény kezelési képzéséhez mélyrehatóbb és valószerűbb környezetet biztosítson.

RE 3. A biztonsági események kezelésének tesztelése
Az érintett szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket kidolgozott tesztek felhasználásával, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket.

RE 3. 1. Egyeztetés
Egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (pl. üzletmenet folytonossági terv és katasztrófa elhárítási terv) felelős szervezeti egységekkel.

RE 4. A biztonsági események kezelése
Az érintett szervezet:
a) eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást;
b) egyezteti az eseménykezelési eljárásokat az üzletmenet folytonossági tervéhez tartozó tevékenységekkel;
c) az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.

RE 4. 1. Automatikus eseménykezelés
Automatizált mechanizmusokat alkalmaz az eseménykezelési eljárások támogatására.

RE 4. 2. Információ korreláció
Összefüggésbe hozza a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat, hogy egy szervezet-szintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és reagálásokra.

RE 5. A biztonsági események figyelése
Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.

RE 5. 1. Automatikus nyomon követés, adatgyűjtés és vizsgálat
Automatizált mechanizmusokat alkalmaz, hogy segítsék a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.

RE 6. A biztonsági események jelentése

Az érintett szervezet:
a) megköveteli, hogy a személyzet jelentse a biztonsági esemény bekövetkeztének gyanúját;
b) jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságnak.

RE 6. 1. Automatizált jelentés
Automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események jelentését.

RE 7. Segítségnyújtás a biztonsági események kezeléséhez
Az érintett szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.

RE 7. 1. Automatizált támogatás
Automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

RE 8. Biztonsági eseménykezelési terv
Az érintett szervezet:
a) kidolgoz egy biztonsági eseménykezelési tervet, amely:
1. Az érintett szervezet számára iránymutatást biztosít a biztonsági esemény kezelési módjaira,
2. ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,
3. átfogó szintű megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,
4. kielégíti a szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit,
5. meghatározza a bejelenteni köteles biztonsági eseményeket,
6. meghatározza és folyamatosan finomhangolja a biztonsági esemény kiértékelésének, kategorizálásának (súlyosság, stb.) kritérium rendszerét,
7. támogatást ad a biztonsági esemény kezelési lehetőségek belső mérésére,
8. meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági esemény kezelési lehetőségek hatékony kidolgozására és fenntartására;
b) kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek;
c) meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet;
d) frissíti a biztonsági eseménykezelési tervet, figyelembe véve a rendszer és szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;
e) a biztonsági eseménykezelési terv változásait b) pont szerint ismerteti;
f) gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, illetve módosítható.

2. melléklet a .../2013. (... ...) NFM rendelethez

Besorolási útmutató

Általános rendelkezések

A szervezet biztonsági szintjét az 1-5. számozású oszlopok jelzik. Az adott oszlopban szereplő:

„0” jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ezen a biztonsági szinten nem kötelező;
X jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ezen a biztonsági szinten kötelező,
X jel és a mögötte levő számérték azt jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ezen a biztonsági szinten kötelező, továbbá azt adott intézkedést az alárendelt kiegészítő eljárások számértékének megfelelően ki kell bővíteni.

A sorrend oszlopban szereplő jelzések az intézkedések megvalósításának sorrendjét jelzik. Az 1-es kódú (P1) intézkedés a legfontosabb, a fontossági sorrend nagyobb jelzőszám irányában csökken. Ebből következik, hogy először azokat az alapvető biztonsági intézkedéseket kell megvalósítani, amelyektől más intézkedések függenek. Ezzel lehetővé téve, hogy a szervezetek az intézkedéseket strukturált eljárással, a rendelkezésre álló erőforrásokkal összhangban alakítsák ki.

Adminisztratív védelmi intézkedések

	A	B	C	D	E	F	G	H
1		**a szervezet biztonsági szintje:**	**1**	**2**	**3**	**4**	**5**	Sorrend
2	**AL**	**Szervezeti szintű alap feladatok**						
3	AL 1.	Informatikai biztonságpolitika	X	X	X	X	X	P1
4	AL 2.	Informatikai biztonsági stratégia	X	X	X	X	X	P1
5	AL 3.	Informatikai biztonsági szabályzat	X	X	X	X	X	P1
6	AL 4.	Az elektronikus információs rendszerek biztonságáért felelős személy	X	X	X	X	X	P1
7	AL 5.	Pénzügyi erőforrások biztosítása	0	X	X	X	X	P1
8	AL 6.	Cselekvési terv és mérföldkövei	0	X	X	X	X	P1
9	AL 7.	Az elektronikus információs rendszerek nyilvántartása	X	X	X	X	X	P1
10	AL 8.	A biztonsági teljesítmény mérése	0	0	X	X	X	P1

11	AL 9.	Szervezet szintű architektúra	0	0	X	X	X	P1
12	AL 10.	Kockázatkezelési stratégia	0	X	X	X	X	P1
13	AL 11.	Biztonság engedélyezési eljárás	X	X	X	X	X	P1
14	AL 12.	Tesztelés, képzés és felügyelet	0	0	X	X	X	P1
15	AL 13.	Kapcsolattartás biztonsági csoportokkal és szervezetekkel	0	0	0	X	X	P1
16	**KE**	**Kockázatelemzés**						
17	KE 1.	Kockázatelemzési eljárásrend	X	X	X	X	X	P1
18	KE 2.	Biztonsági osztályba sorolás	X	X	X	X	X	P1
19	KE 3.	Kockázatelemzés	X	X	X	X	X	P1
20	KE 4.	Sebezhetőség vizsgálat	0	0	X	X(1-3)	X(1-4)	P1
21	**TE**	**Tervezés**						
22	TE 1.	Biztonsági tervezési eljárásrend	0	X	X	X	X	P1
23	TE 2.	Rendszerbiztonsági terv	0	X	X	X(1)	X(1)	P1
24	TE 3.	Viselkedési szabályok	0	X	X	X(1)	X(1)	P1
25	TE 4.	Információbiztonsági architektúra leírás	0	0	0	X	X	P1
26	**RB**	**Rendszer és szolgáltatás beszerzés**						
27	RB 1.	Beszerzési eljárásrend	0	X	X	X	X	P1
28	RB 2.	Erőforrás kiosztás	0	0	X	X	X	P1
29	RB 3.	A rendszer fejlesztés életciklusa	0	X	X	X	X	P1
30	RB 4.	Beszerzések	0	0	X	X(1-3)	X(1-3)	P1
31	RB 5.	Az elektronikus információs rendszerre vonatkozó dokumentáció	0	0	X	X	X	P2
32	RB 6.	Biztonságtervezési elvek	0	0	0	X	X	P1
33	RB 7.	Külső elektronikus információs rendszerek szolgáltatásai	0	X	X	X(1)	X(1)	P1
34	RB 8.	Fejlesztői konfigurációkezelés	0	0	0	X	X	P1

35	RB 9.	Fejlesztői biztonsági tesztelés	0	0	0	X	X	P2
36	RB 10.	Beszerzés védelem	0	0	0	0	X	P1
37	RB 11.	Fejlesztési folyamat, szabványok és eszközök	0	0	0	0	X	P2
38	RB 12.	Fejlesztői oktatás	0	0	0	0	X	P2
39	RB 13.	Fejlesztői biztonsági architektúra és tervezés	0	0	0	0	X	P1
40	**BE**	**Biztonsági értékelés**						
41	BE 1.	Biztonságértékelési eljárásrend	0	0	X	X	X	P1
42	BE 2.	Biztonsági értékelések	0	0	X	X(1)	X(1-2)	P2
43	BE 3.	Az elektronikus információs rendszer kapcsolódásai	0	0	X	X(1)	X(1)	P1
44	BE 4.	Cselekvési terv	0	0	X	X	X	P3
45	BE 5.	Folyamatos ellenőrzés	0	0	X	X(1)	X(1)	P3
46	BE 6.	Áthatolás tesztelés	0	0	0	0	X	P1
47	BE 7.	Belső rendszer kapcsolatok	0	0	X	X	X	P1
48	**SZ**	**Emberi tényezőket figyelembe vevő – személy – biztonság**						
49	SZ 1.	Személybiztonsági eljárásrend	0	0	X	X	X	P1
50	SZ 2.	Munkakörök, feladatok biztonsági szempontú besorolása	0	0	X	X	X	P1
51	SZ 3.	A személyek ellenőrzése	0	0	X	X	X	P1
52	SZ 4.	Eljárás jogviszony megszűnésekor	X	X	X	X	X(1)	P2
53	SZ 5.	Áthelyezések, átirányítások és kirendelések kezelése	0	0	X	X	X	P2
54	SZ 6.	Szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények	0	0	X	X	X	P1
55	SZ 7.	Fegyelmi intézkedések	X	X	X	X	X	P3
56	**TK**	**Tudatosság és képzés**						
57	TK 1	Képzési eljárásrend	X	X	X	X	X	P1

58	TK 2.	Biztonság tudatosság képzés	X	X	X	X(1)	X(1)	P1
59	TK 3.	Szerepkör alapú biztonsági képzés	0	0	X	X	X	P1
60	TK 4.	A biztonsági képzésre vonatkozó jegyzőkönyvek	0	0	X	X	X	P3

Fizikai védelmi intézkedések

	A	B	C	D	E	F	G	H
1		**a szervezet biztonsági szintje:**	1	2	3	4	5	Sorrend
2	FK 1.	Fizikai védelmi eljárásrend	0	X	X	X	X	P1
3	FK 2.	Fizikai belépési engedélyek	0	X	X	X	X	P1
4	FK 3.	A fizikai belépés ellenőrzése	0	X	X	X	X(1)	P1
5	FK 4.	Hozzáférés az elosztási és átviteli vonalakhoz	0	0	0	X	X	P1
6	FK 5.	A kimeneti eszközök hozzáférés ellenőrzése	0	0	0	X	X	P1
7	FK 6.	A fizikai hozzáférések felügyelete	0	0	X	X(1)	X(1-2)	P1
8	FK 7.	A látogatók ellenőrzése	0	0	X	X	X(1)	P3
9	FK 8.	Áramellátó berendezések és kábelezés	0	0	0	X	X	P1
10	FK 9.	Vészkikapcsolás	0	0	0	X	X	P1
11	FK 10.	Tartalék áramellátás	0	0	0	X	X(1)	P1
12	FK 11.	Vészvilágítás	0	0	X	X	X	P1
13	FK 12.	Tűzvédelem	0	0	X	X(1)	X(1-3)	P1
14	FK 13.	Hőmérséklet és páratartalom ellenőrzés	0	0	X	X	X	P1
15	FK 14.	Vízkár elleni védelem	0	0	X	X	X(1)	P1
16	FK	Be és kiszállítás	0	0	X	X	X	P1

	15.							
17	FK 16.	Tartalék munkahelyszínek	0	0	0	X	X	P1
18	FK 17.	Az elektronikus információs rendszer elemeinek elhelyezése	0	0	0	X	X	P2

Logikai védelmi intézkedések

	A	B												C
		B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	
1		**elektronikus információs rendszer biztonsági osztályba sorolása**												Sorrend
2		**Bizalmasság (C)**				**Sértetlenség (I)**				**Rendelkezésre állás (A)**				
3		**2**	**3**	**4**	**5**	**2**	**3**	**4**	**5**	**2**	**3**	**4**	**5**	
4	**KK**	**Konfigurációkezelés**												
5	KK 1.	X	X	X	X	X	X	X	X	X	X	X	X	P1
6	KK 2.	X	X	X(1-3)	X(1-4)	X	X	X(1-3)	X(1-4)	X	X	X(1-3)	X(1-4)	P1
7	KK 3.	0	X	X(1)	X(1-2)	0	X	X(1)	X(1-2)	0	X	X(1)	X(1-2)	P1
8	KK 4.	0	X	X	X(1)	0	X	X	X(1)	0	X	X	X(1)	P2
9	KK 5.	0	0	0	0	0	0	X	X(1-3)	0	0	0	0	P1
10	KK 6.	0	X	X	X(1-2)	0	X	X	X(1-2)	0	X	X	X(1-2)	P1
11	KK 7.	0	X	X(1-3)	X(1-2),4	0	X	X(1-3)	X(1-2),4	0	X	X(1-3)	X(1-2),4	P1
12	KK 8.	X	X	X(1-3)	X(1-5)	X	X	X(1-3)	X(1-5)	X	X	X(1-3)	X(1-5)	P1
13	KK 9.	0	0	X	X	0	0	X	X	0	0	X	X	P1
14	KK 10.	X	X	X	X	X	X	X	X	X	X	X	X	P1
15	KK 11.	X	X	X	X	X	X	X	X	X	X	X	X	P1
16	**UF**	**Üzletmenet folytonosság tervezése**												
17	ÜF 1.	0	0	0	0	0	0	0	0	X	X	X	X	P1
18	ÜF 2.	0	0	0	0	0	0	0	0	X	X	X(1-3)	X(1-6)	P1
19	ÜF 3.	0	0	0	0	0	0	0	0	0	X	X	X(1)	P2
20	ÜF 4.	0	0	0	0	0	0	0	0	0	0	X(1)	X(1-2)	P2
21	ÜF 5.	0	0	0	0	0	0	0	0	0	0	X(1-2)	X(1-3)	P1
22	ÜF 6.	0	0	0	0	0	0	0	0	0	0	X(1-3)	X(1-4)	P1
23	ÜF 7.	0	0	0	0	0	0	0	0	0	0	X(1-2)	X(1-2)	P1

24	ÜF 8.	0	0	0	0	X	X	X(1)	X(1)	X	X	X(1)	X(1-4)	P1
25	ÜF 9.	0	0	0	0	X	X	X(1)	X(1)	X	X	X(1)	X(1-2)	P1
26	**KA**	**Karbantartás**												
27	KA 1.	0	0	0	0	X	X	X	X	X	X	X	X	P1
28	KA 2.	0	0	0	0	X	X	X	X(1)	X	X	X	X(1)	P2
29	KA 3.	0	0	0	0(3)	0	0	X(1-2)	X(1-2)	0	0	X(1-2)	X(1-2)	P2
30	KA 4.	0	0	X(1)	X(1-2)	0	0	X(1)	X(1-2)	0	0	X(1)	X(1-2)	P1
31	KA 5.	0	X	X	X(1)	0	X	X	X(1)	0	X	X	X(1)	P1
32	KA 6.	0	0	0	0	0	0	0	0	0	0	X	X	P1
33	**AV**	**Adathordozók védelme**												
34	AV 1	X	X	X	X	X	X	X	X	X	X	X	X	P1
35	AV 2.	X	X	X	X	X	X	X	X	X	X	X	X	P1
36	AV 3.	0	0	X	X	0	0	0	0	0	0	0	0	P1
37	AV 4.	0	0	X	X	0	0	0	0	0	0	0	0	P1
38	AV 5.	0	0	X(1)	X(1)	0	0	X(1)	X(1)	0	0	X	X	P1
39	AV 6.	X	X	X	X(1-3)	0	0	0	0	0	0	0	0	P1
40	AV 7.	X	X	X(1)	X(1)	X	X	X(1)	X(1)	X	X	X(1)	X(1)	P1
41	**AH**	**Azonosítás és hitelesítés**												
42	AH 1.	X	X	X	X	X	X	X	X	X	X	X	X	P1
43	AH 2.	X	X(1)	X(1-5)	X(1-7)	X	X(1)	X(1-5)	X(1-7)	X	X(1)	X(1-5)	X(1-7)	P1
44	AH 3.	0	0	X	X	0	0	X	X	0	0	X	X	P1
45	AH 4.	X	X	X	X	X	X	X	X	X	X	X	X	P1
46	AH 5.	X	X(1-2)	X(1-4)	X(1-4)	X	X(1-2)	X(1-4)	X(1-4)	X	X(1-2)	X(1-4)	X(1-4)	P1
47	AH 6.	X	X	X	X	X	X	X	X	X	X	X	X	P1
48	AH 7.	0	X	X	X	0	X	X	X	0	X	X	X	P1
49	AH 8.	X	X(1)	X(1)	X(1)	X	X(1)	X(1)	X(1)	X	X(1)	X(1)	X(1)	P1
50	**HE**	**Hozzáférés ellenőrzése**												
51	HE 1.	X	X	X	X	X	X	X	X	X	X	X	X	P1
52	HE 2 .	X	X	X(1-4)	X(1-7)	X	X	X(1-4)	X(107)	X	X	X(1-4)	X(1-7)	P1

53	HE 3.	X	X	X	X	X	X	X	X	X	X	X	X	P1
54	HE 4.	0	0	X	X	0	0	X	X	0	0	X	X	P1
55	HE 5.	0	0	X	X	0	0	X	X	0	0	X	X	P1
56	HE 6.	0	0	X(1-5)	X(1-6)	0	0	X(1-5)	X(1-6)	0	0	X(1-5)	X(1-6)	P1
57	HE 7.	0	X	X	X	0	X	X	X	0	X	X	X	P2
58	HE 8.	0	X	X	X	0	X	X	X	0	X	X	X	P1
59	HE 9.	0	0	0	X	0	0	0	X	0	0	0	X	P2
60	HE 10.	0	0	X(1)	X(1)	0	0	X(1)	X(1)	0	0	X(1)	X(1)	P3
61	HE 11.	0	0	X	X	0	0	X	X	0	0	X	X	P2
62	HE 12.	X	X	X	X	X	X	X	X	X	X	X	X	P1
63	HE 13.	0	X	X(1-4)	X(1-4)	0	X	X(1-4)	X(1-4)	0	X	X(1-4)	X(1-4)	P1
64	HE 14.	0	X	X(1)	X(1-3)	0	X	X(1)	X(1-3)	0	X	X(1)	X(1-3)	P1
65	HE 15.	0	X	X(1)	X(1)	0	X	X(1)	X(1)	0	X	X	X	P1
66	HE 16	X	X	X(1-2)	X(1-2)	X	X	X(1-2)	X(1-2)	X	X	X(1-2)	X(1-2)	P1
67	HE 17.	0	0	X	X	0	0	0	0	0	0	0	0	P2
68	HE 18.	X	X	X	X	X	X	X	X	X	X	X	X	P2
69	**NA**	**Naplózás és elszámoltathatóság**												
70	NA 1.	X	X	X	X	X	X	X	X	X	X	X	X	P1
71	NA 2.	X	X	X	X(1)	X	X	X	X(1)	X	X	X	X(1)	P1
72	NA 3.	X	X	X(1)	X(1-2)	X	X	X(1)	X(1-2)	X	X	X(1)	X(1-2)	P1
73	NA 4.	0	X	X	X	0	X	X	X	0	X	X	X	P1
74	NA 5.	0	X	X	X(1-2)	0	X	X	X(1-2)	0	X	X	X(1-2)	P1
75	NA 6.	0	X	X(1-2)	X(1-4)	0	X	X(1-2)	X(1-4)	0	X	X(1-2)	X(1-4)	P1
76	NA 7.	0	0	X(1)	X(1)	0	0	X(1)	X(1)	0	0	X(1)	X(1)	P2
77	NA 8.	X	X	X(1)	X(1)	X	X	X(1)	X(1)	X	X	X(1)	X(1)	P1
78	NA 9.	X	X	X(1)	X(1-2)	X	X	X(1)	X(1-3)	X	X	X(1)	X(1-2)	P1
79	NA 10.	0	0	0	X	0	0	0	X	0	0	0	X	P1
80	NA 11.	X	X	X	X	X	X	X	X	X	X	X	X	P3
81	NA 12.	X	X	X	X(1-2)	X	X	X	X(1-2)	X	X	X	X(1-2)	P1
82	**RS**	**Rendszer és információ sértetlenség**												
83	RS 1.	0	0	0	0	X	X	X	X	0	0	0	0	P1
84	RS 2.	0	0	0	0	X	X	X(1)	X(1-2)	0	0	0	0	P1

85	RS 3.	X	X	X(1-2)	X(1-2)	X	X	X(1-2)	X(1-2)	X	X	X(1-2)	X(1-2)	P1
86	RS 4.	X	X	X(1-3)	X(1-3)	X	X	X(1-3)	X(1-3)	X	X	X(1-3)	X(1-3)	P1
87	RS 5.	0	X	X	X(1)	0	X	X	X(1)	0	X	X	X(1)	P1
88	RS 6.	0	0	0	X	0	0	0	X	0	0	0	0	P1
89	RS 7.	0	0	X(1-2)	X(1-5)	0	0	X(1-2)	X(1-5)	0	0	X(1-2)	X(1-5)	P1
90	RS 8.	0	0	0	0	0	0	X(1-2)	X(1-2)	0	0	0	0	P1
91	RS 9.	0	0	0	0	0	0	X	X	0	0	0	0	P1
92	RS 10.	0	0	0	0	0	0	X	X	0	0	0	0	P2
93	RS 11.	X	X	X	X	X	X	X	X	0	0	0	0	P2
94	RS 12.	0	0	X	X	0	0	X	X	0	0	X	X	P1
95	**RV**	**Rendszer és kommunikáció védelem**												
96	RV 1.	X	X	X	X	X	X	X	X	X	X	X	X	P1
97	RV 2.	0	0	X	X	0	0	X	X	0	0	X	X	P1
98	RV 3.	0	0	0	X	0	0	0	X	0	0	0	X	P1
99	RV 4.	0	0	X	X	0	0	0	0	0	0	0	0	P1
100	RV 5.	0	0	0	0	0	0	0	0	0	X	X	X	P1
101	RV 6.	X	X	X(1-4)	X(1-7)	X	X	X(1-4)	X(1-7)	X	X	X(1-4)	X(1-7)	P1
102	RV 7.	0	0	X(1)	X(1)	0	0	0	0	0	0	0	0	P1
103	RV 8.	0	0	0	0	0	0	X(1)	X(1)	0	0	0	0	P1
104	RV 9.	0	0	0	0	0	0	0	0	0	0	X	X	P2
105	RV 10.	X	X	X	X(1)	X	X	X	X(1)	X	X	X	X(1)	P1
106	RV 11.	X	X	X	X	X	X	X	X	0	0	0	0	P1
107	RV 12.	X	X	X	X	0	0	0	0	0	0	0	0	P1
108	RV 13.	0	0	X	X	0	0	X	X	0	0	0	0	P1
109	RV 14.	0	0	X	X	0	0	X	X	0	0	0	0	P1
110	RV 15.	0	0	X	X	0	0	0	0	0	0	0	0	P1
111	RV 16.	0	0	0	0	0	X	X	X	0	0	0	0	P1
112	RV 17.	0	0	0	0	0	X	X	X	0	0	0	0	P1

113	RV 18.	0	0	0	0	0	X	X	X	0	0	0	0	P1
114	RV 19.	0	0	0	0	0	0	X	X	0	0	0	0	P1
115	RV 20.	0	0	0	X	0	0	0	X	0	0	0	X	P1
116	RV 21.	0	0	X	X	0	0	X	X	0	0	0	0	P1
117	RV 22.	X	X	X	X	X	X	X	X	0	0	0	0	P1
118	**RE**	**Reagálás a biztonsági eseményekre**												
119	RE 1.	0	X	X	X	0	X	X	X	0	X	X	X	P1
120	RE 2.	0	X	X	X(1-2)	0	X	X	X(1-2)	0	X	X	X(1-2)	P2
121	RE 3.	0	0	X(1)	X(1)	0	0	X(1)	X(1)	0	0	X(1)	X(1)	P2
122	RE 4.	0	X	X(1)	X(1-2)	0	X	X(1)	X(1-2)	0	X	X(1)	X(1-2)	P1
123	RE 5.	0	X	X	X(1)	0	X	X	X(1)	0	X	X	X(1)	P1
124	RE 6.	0	X	X(1)	X(1)	0	X	X(1)	X(1)	0	X	X(1)	X(1)	P1
125	RE 7.	0	X	X(1)	X(1)	0	X	X(1)	X(1)	0	X	X(1)	X(1)	P3
126	RE 8.	0	X	X	X	0	X	X	X	0	X	X	X	P1

3. melléklet a .../2013. (... ...) NFM rendelethez

Az elektronikus információs rendszerek biztonsági osztályba sorolásának szempontjai

1. Az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából az alábbi irányelvek szerint kell elvégezni, figyelemmel arra is, hogy egyes elektronikus információs rendszerek tekintetében funkciójukból adódóan kiemelten az egyik szempontot kell erőteljesen érvényesíteni, így például

- a minősített információt kezelő rendszerek, ahol elsősorban a bizalmassági követelmény teljesítése az elsődleges elvárás (ennek a magas színvonalú intézkedésekkel történő biztosítása általában a sértetlenségi elvárás teljesülését is garantálhatja, de a rendelkezésre állást nem);
- a nemzeti adatvagyont kezelő rendszerek esetében kiemelt a sértetlenség követelménye;
- a létfontosságú információs rendszerelemek (infrastruktúra) esetében elsősorban a rendelkezésre állás követelménye a jellemző elvárás.

2. Az elektronikus információs rendszerben kezelt adatok alapján meg kell különböztetni az alábbi adattípusokat:

a) Nemzeti vagy külföldi minősített adatok, melyekre a minősített adat védelméről szóló 2009. évi CLV. törvény (továbbiakban: MAVtv) rendelkezéseit az irányadóak.
b) Nem minősített adatok.

3. Az elektronikus információs rendszerek biztonsági osztályba sorolását kockázatelemzés alapján kell elvégezni, és azt a szervezet vezetője hagyja jóvá. Az osztályba sorolást megelőző kockázatelemzés során ajánlott nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembe vétele. A kockázatelemezés alapját az adatok és az adott információs rendszer jellegéből kiindulva

a) az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, illetve az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár nagysága;
b) illetve a kár bekövetkezésének becsült valószínűsége

képzi.

A biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárérték, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárnagyságot kell, vagy lehet figyelembe venni, a szervezet döntésétől függően.

4. Az elektronikus információs rendszerek biztonsági osztályai meghatározásához az alábbi – az érintett szervezet szempontjából szóba jöhető – kártípusokat kell többek között figyelembe venni:

a) minősített adatok bizalmasságának (esetleg sértetlenségének vagy rendelkezésre állásának) elvesztése;
b) társadalmi-politikai, illetve a jog sérüléséből adódó hatások (pl. alaptevékenységek akadályozása, különösen a létfontosságú információs rendszerelemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, közérdekű adatok titokban tartása, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, jogsértés);
c) személyeket, csoportokat érintő károk (pl. nem nyilvános személyes adatok – ilyenek az egészségügyi adatok, banktitkok - megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések veszélye),
d) közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, illetve ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, üzleti titkok megsértése, adatok sértetlenségének, rendelkezésre állásának elvesztése),
e) közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).

5. A biztonsági osztályok és a releváns, valamilyen eséllyel előforduló káreseményekhez tartozó irányadó kárérték szintek besorolási ajánlásai a bizalmasság, sértetlenség és rendelkezésre állás szerint külön-külön értékelendők a következő elvek figyelembe vételével. Az Ibtv. szerint a besorolás elvégzése az érintett szervezet felelőssége, az alábbiak a döntéshez csak szempontokat jelentenek:

1. biztonsági osztály
Csak jelentéktelen káresemény következhet be, azaz:
a) a rendszer nem kezel minősített, vagy más, jogszabályok által védett (pl.: személyes) adatot;
b) nincs bizalomvesztés, a probléma kisebb, szervezeten belül marad, és azon belül meg is oldható,
c) a közvetlen és közvetett anyagi kár a szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentéktelen.

2. biztonsági osztály
Csekély káresemény következhet be, azaz:
a) "Korlátozott terjesztésű!" adat bizalmassága sérülhet,
b) néhány személyes adat bizalmassága vagy hitelessége sérülhet,
c) csekély értékű üzleti titkot képző, vagy belső (intézményi) szabályzóval védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérülhet,
d) a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető,
e) a közvetlen és közvetett anyagi kár a szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély,

3. biztonsági osztály
Közepes káresemény következhet be, azaz:
a) „Bizalmas!” adat bizalmassága sérülhet,

b) egyedi személyes adatok bizalmassága, sértetlensége, vagy rendelkezésre állása nagyobb számban sérülhet,
c) közepes értékű üzleti titkot, vagy a szervezet szempontjából érzékeny információt képző vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérülhet,
d) a lehetséges társadalmi-politikai hatás: bizalomvesztés a szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülnek,
e) a közvetlen és közvetett anyagi kár a szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest közepes.

4. biztonsági osztály
Nagy káresemény következhet be, azaz:

a) „Titkos!” adat bizalmassága sérülhet,
b) különleges személyes adatok, nagy tömegű személyes adat bizalmassága vagy sértetlensége, rendelkezésre állása sérülhet,
c) személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatt veszélyeket),
d) nagy értékű, üzleti titkot, vagy a szervezet szempontjából különösen érzékeny információt képző adat bizalmassága, sértetlensége, vagy rendelkezésre állása tömegesen sérülhet,
e) a káresemény lehetséges társadalmi-politikai hatása a bizalomvesztés a szervezeten belül, jogszabályok betartása sérülhet, bizalomvesztés a szervezet felső vezetésében, a középvezetésen belül személyi konzekvenciák,
f) a közvetlen és közvetett anyagi kár a szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős,

5. biztonsági osztály
Kiemelkedően nagy káresemény következhet be, azaz:

a) „Szigorúan titkos!” adat bizalmassága sérülhet,
b) nagy tömegű különleges személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
c) személyi sérülések nagy számban következhetnek be,
d) a nemzeti adatvagyon helyreállítható sértetlensége nem biztosított,
e) létfontosságú információs rendszerelem megfelelő szintű rendelkezésre állása nem biztosított,
f) társadalmi-politikai hatás: súlyos bizalomvesztés a szervezettel szemben, jelentős jogsértések következhetnek be,
g) a közvetlen és közvetett anyagi kár a szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős, nagy értékű üzleti titok, a szervezet szempontjából kiemelten érzékeny információt képező adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

4. melléklet a .../2013. (... ...) NFM rendelethez

Az elektronikus információs rendszereket működtető szervezetek biztonsági szintbe sorolásának szempontjai

A szervezet biztonsági szintjét – az Ibtv 9.§ (2) pontja mellett - meghatározza a működtetett elektronikus információs rendszerek biztonsági osztályba sorolása. Az érintett szervezetek biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos, vagy magasabb besorolású, de a szervezettől függően legalább az Ibtv. 9.§ (2) pontja szerinti. A tv. 9.§ (4) pontja szerint indokolt esetben a reá vonatkozónál alacsonyabb biztonsági szint is megállapítható.

A szervezet biztonsági szintjeinek az alábbi, fokozatosan szigorodó biztonsági jellemzői vannak.

A szervezet biztonsági szintje 1. ha a szervezet által működtetett elektronikus információs rendszerek esetén nincs 1. biztonsági osztálynál magasabb besorolású rendszer, és a szervezet vezetői döntése alapján elfogadható az, hogy az elektronikus információbiztonsági folyamatai kezdeti, ad hoc jellegűek, azaz:

a) a szervezetnél a biztonsági folyamatoknak nincsenek átfogó részletszabályai, azokat az elfogadott magas szintű szabályzatok (Informatikai biztonsági politika, Informatikai biztonsági stratégia, valamint Informatikai biztonsági szabályzat) szabályozzák;
b) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket és feladatokat egy, az elektronikus információs rendszer biztonságáért felelős személyhez rendelték hozzá, akinek irányítási jogköre korlátozott;
c) az elektronikus információs rendszerek biztonsága az egyének tudatosságán múlik,
d) az elektronikus információs rendszerek biztonságával megkésve, az eseményekre reagálva foglalkoznak;
e) az elektronikus információs rendszerek biztonságát nem mérik,
f) az észlelt biztonsági szabálysértések esetén a felelős kiléte nem állapítható meg, mert a felelősségi körök nincsenek egyértelműen tisztázva;
g) a működtetett rendszer és a kezelt adatok védelme különleges fizikai védelmi intézkedéseket nem igényelnek.

A szervezet biztonsági szintje 2. ha a szervezet által működtetett elektronikus információs rendszerek esetén nincs 2. biztonsági osztálynál magasabb besorolású rendszer, és a szervezet vezetői döntése alapján elfogadható az, hogy a szervezet informatikai folyamatai részben szabályozottak, azaz:

a) a szervezetnél a biztonsági folyamatoknak nincsenek átfogó részletszabályai, azokat az elfogadott magas szintű szabályzatok (Informatikai biztonsági politika, Informatikai biztonsági stratégia, valamint Informatikai biztonsági szabályzat, valamint a tervezésre, beszerzésre, fejlesztésre, képzésre vonatkozó szakterületi belső előírások) szabályozzák;
b) az elektronikus információs rendszerek biztonsági szabályzataihoz kapcsolatos eljárások kidolgozása folyamatban van, de sem megfelelő szaktudás, sem megfelelő eszközrendszer nem áll rendelkezésre;
c) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket és feladatokat egy, az elektronikus információs rendszer biztonságáért felelős személyhez rendelték hozzá, akinek irányítási jogköre korlátozott;
d) az elektronikus információs rendszerek előállítanak biztonságra vonatkozó információkat, de azokat nem elemzik;
e) az elektronikus információs rendszerek biztonságára vonatkozó jelentések nem teljes körűek,
f) az elektronikus információs rendszerek biztonságára nem a szervezet teljes körű biztonságának részeként, hanem elsősorban az informatika belső felelősségeként, területeként kezelik;
g) a fizikai beléptetés ellenőrzésén túlmenően a működtetett rendszer és a kezelt adatok védelme további fizikai védelmi intézkedéseket nem igényelnek.

A szervezet biztonsági szintje 3. ha a szervezet által működtetett elektronikus információs rendszerek esetén nincs 3. biztonsági osztálynál magasabb besorolású rendszer, és a szervezet vezetői döntése alapján elvárt, hogy a szervezet elektronikus információbiztonsági folyamatai jól szabályozottak legyenek, a folyamatokat dokumentálják és az adminisztratív védelmi intézkedéseket hatékony logikai védelmi intézkedésekkel támogassák, azaz:

a) az elektronikus információs rendszerek biztonsági eljárásait meghatározták, és azokat összehangolták a biztonságpolitikával, stratégiával, szabályzattal;
b) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket meghatározták, és azokat az érintettek ismerik;
c) a kockázatelemzés eredményeit figyelembe vették a biztonsági megoldások kidolgozásánál;
d) a biztonságirányítási célokat és mérési módszereket meghatározták, de még nem teljes körűen mérik;
e) ad hoc jellegű biztonsági tesztelést és sebezhetőség vizsgálatot végeznek;
f) a biztonságtudatosságot megteremtették, és azt a vezetés támogatja, a biztonsági képzés az informatika és az általános szakmai területei rendelkezésére áll, de az ütemezése és a megtartása nem formalizált;
g) a fizikai védelmi intézkedések kiterjednek az információs rendszerelemekhez történő fizikai hozzáférések felügyeletére és további védelmi eszközök alkalmazásával a rendszer fizikai egységeit védik a különböző fizikai károk ellen;
h) tartalék munkahelyek vannak kialakítva;
i) az elektronikus információs rendszerek fejlesztésénél törekednek az integrált elektronikus információs rendszer biztonsági értékelésére vagy tanúsítására.

A szervezet biztonsági szintje 4. ha a szervezet által működtetett elektronikus információs rendszerek esetén nincs 4. biztonsági osztálynál magasabb besorolású rendszer, valamint a szervezet vezetői döntése alapján elvárt, hogy a szervezet elektronikus információbiztonsági folyamatai irányítottak és mérhetőek legyenek, azaz:

a) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségi köröket egyértelműen meghatározták, menedzselik és betartatják;
b) a biztonsági kockázat- és hatáselemzés végrehajtása következetes;
c) a felhasználói azonosítás, hitelesítés és jogosultság engedélyezés szabványosított,
d) törekszenek arra, hogy a biztonsági auditálásért és irányításért felelős munkatársak elektronikus információs rendszerek biztonságához kapcsolódó szerepkör alapú szakmai képesítést szerezzenek meg,
e) a biztonság tesztelését szabványos és formális folyamatok felhasználásával végzik, amelyek eredményeképpen a biztonsági szintek javulnak;
f) az elektronikus információs rendszerek biztonsági folyamatait összehangolják a szervezet általános biztonsági funkcióival;
g) a biztonság tudatosítását elősegítő módszerek alkalmazása kötelező, az információbiztonsági képzést mind a szervezet általános szakmai, mind az informatikai részlegeinél megtartják;
h) a biztonságirányítás hatékonyságát mérik és tájékoztatást adnak az eredményekről;
i) a fizikai védelmi intézkedések kiterjednek az információs rendszerelemekhez történő fizikai hozzáférések felügyeletére és további védelmi eszközök alkalmazásával a rendszer fizikai egységeit védik fizikai károk ellen,
j) tartalék munkahelyek kialakításával és az elektronikus információs rendszer elemeinek biztonságos elhelyezésével minimalizálják a lehetséges károkat;
k) a legalább 4. biztonsági osztálynak megfelelő besorolású elektronikus információs rendszerek üzembeállítását megelőzi a teljes rendszer független, külső (úgynevezett fekete dobozos) sebezhetőség-vizsgálaton alapuló, pozitív eredményű (csak a szervezet által elfogadható maradványkockázatokat tartalmazó) legalább fokozott garanciaszintű rendszerértékelése vagy tanúsítása.
l) az elektronikus információs rendszer fejlesztésénél törekednek széleskörűen elterjedt, lehetőleg biztonsági szempontból értékelt termékek beszerzésére. A biztonsági funkciók beépítésének szükségét figyelembe veszik az alkalmazások tervezési, fejlesztési, beszerzési, felhasználási és üzemeltetési folyamataiba egyaránt.

A szervezet biztonsági szintje 5. ha a szervezet által működtetett elektronikus információs rendszerek esetén van 5. biztonsági osztályú besorolású rendszer, valamint a szervezet vezetői döntése alapján elvárt, hogy a szervezet elektronikus információbiztonsági folyamatai optimalizáltak legyenek, a máshol már bevált gyakorlatokat kövessék, és azokat automatizálják, azaz:

a) az elektronikus információs rendszerek biztonsága a szakmai és az informatikai vezetés közös felelőssége, és integrálva van a szervezeti biztonság szakmai célkitűzéseivel,
b) az elektronikus információs rendszerek biztonsági követelményeit egyértelműen meghatározták, optimalizálták és beépítették a jóváhagyott rendszerbiztonsági tervbe,
c) a felhasználók felelősek a biztonsági követelmények meghatározásáért, és a biztonsági elvárásokat és funkciókat figyelembe veszik már az alkalmazási rendszerek tervezési szakaszában,
d) a biztonsági rendkívüli eseményekkel haladéktalanul, automatizált eszközökkel támogatott, formalizált, rendkívüli helyzetkezelési eljárások segítségével foglalkoznak,
e) rendszeresen biztonsági felméréseket végeznek a rendszerbiztonsági terv megvalósítása eredményességének értékelése céljából,
f) a fenyegetésekre és sebezhetőségekre vonatkozó információkat rendszeresen begyűjtik és elemzik,
g) a kockázatok enyhítésére irányuló kontroll folyamatokat alkalmaznak, hatékonyságukat rendszeresen elemzik,
h) a biztonsági folyamatok folyamatos javítása érdekében felhasználják a biztonsági tesztelést, a rendkívüli biztonsági események feltáró elemzését és a kockázatok felismerését aktívan kezdeményezik,
i) a vezetés előbbi mutatókat felhasználja a rendszerbiztonsági terv folyamatos javítási folyamat keretében történő kiegészítésére,
j) a fizikai védelmi intézkedések kiterjednek az információs rendszerelemekhez történő fizikai hozzáférések felügyeletére és további védelmi eszközök alkalmazásával a rendszer fizikai egységeit védik a fizikai károk ellen, valamint tartalék munkahelyek kialakításával minimalizálják a lehetséges károkat;
k) a legalább 5. biztonsági osztálynak megfelelő besorolású elektronikus információs rendszerek fejlesztésénél széleskörűen elterjedt, biztonsági szempontból értékelt termékek kerülnek beszerzésére, rendszerbe integrálásra, valamint az integrált rendszer független, külső és belső (fekete és fehér dobozos) sebezhetőség-vizsgálaton alapuló pozitív eredményű, kiemelt garanciaszintű rendszerértékelésre vagy tanúsításra kerül.
l) A biztonsági funkciók beépítését megkövetelik az alkalmazások tervezési, fejlesztési, beszerzési, felhasználási és üzemeltetési folyamatai során egyaránt.

5. melléklet a .../2013. (... ...) NFM rendelethez

Nemzeti Távközlési Gerinchálózat biztonsági jellemzői

1. A Nemzeti Távközlési Gerinchálózat (NTG) Magyarország közigazgatási intézményeinek működését támogató korszerű, IP alapú, integrált hang, adat, multimédia átvitelére alkalmas infokommunikációs hálózat.

2. Az NTG üzemeltetőjének az alábbi jellemzőket és képességeket kell fenntartani és biztosítani.

a) Az NTG országos kiterjedésű, gyűrűs felépítésű, nagysebességű optika gerinchálózatból, gerinchálózati csomópontokból és az intézményi végpontokat elérő felhordóhálózati szakaszokból áll.
b) Az NTG-n biztosított összeköttetések OSI L3 Ethernet interfészek között tetszőleges számú és földrajzi elhelyezkedésű pontot kapcsolnak védett virtuális hálózatba (továbbiakban:VPN). A VPN-ek az IP gerinchálózaton MPLS protokoll használatával kialakított, szükség esetén további titkosítással (IP Sec, SSL) védett csatornákon nyújtanak magas minőségű adatátviteli szolgáltatást végponttól-végpontig.
c) Az NTG nyilvános célú hálózatok felé irányuló kapcsolódásának kialakítása egységesített, ellenőrzött módon, egyetlen-egy ponton keresztül történik. A nyílt internet felé irányuló aggregált intézményi forgalmakat a központi Határvédelmi Rendszer (HVR) felügyeli, melyet az NTG üzemeltető üzemeltet 7X24X365 állandó felügyelet mellett.”

3. Az NTG üzemeltetője az Általános Szerződési Feltételekben (továbbiakban: ÁSZF) jelen rendelet hatályba lépését követő hat hónapon belül közzéteszi, és folyamatosan karbantartja.

3.1.. Az ÁSZF-ben meg kell határozni az NTG szolgáltatásait nyújtó, üzemeltető, felügyelő és igénybevevő szervezetekkel szemben támasztott biztonsági követelményeket, feladatokat és felelősségeket a

a) NTG alaphálózati szolgáltató feladata és felelőssége
b) NTG alaphálózat fejlesztőjének feladata és felelőssége
c) NTG üzemeltető feladata és felelőssége
d) NTG felhasználó kötelezettsége és felelőssége
e) NTG felügyelő feladata és felelőssége

körében.

3.2.. Az NTG üzemeltetője az incidenskezeléssel kapcsolatos eljárásrendet az ÁSZF incidenskezelési mellékletében rögzíti. Az ÁSZF a kiszolgált intézményi kör részére publikusan elérhető interneten a http://nisz.hu oldalon, illetve az ÁSZF-ben történő változásokról az NTG üzemeltető az érintett szervezeteket elektronikus levélben tájékoztatja.

4. Az NTG felhasználó szervezet az NTG-re érvényes biztonsági követelményeket köteles betartani. Minden NTG felhasználó nyilatkozni köteles a közzétett biztonsági követelmények megfelelőségéről saját és a felügyelete alá tartozó szervezet(ei) tekintetében.

5. Az NTG üzemeltetője jogosult és köteles az NTG hálózati forgalmának rendszeres minőségi, mennyiségi és biztonsági ellenőrzésére az NTG működésének folyamatos biztonságos és megfelelő szinten tartása, valamint az ÁSZF keretén belül az egyedi rendelkezésre állási és más szolgáltatásnyújtási feltételeket tartalmazó Szolgáltatási Szint Megállapodásban foglaltak szerint.

6. Az NTG üzemeltetője jogosult az NTG-ből

6.1. Az érintett szervezet és a Nemzeti Elektronikus Információvédelmi Hatóság, illetve a kormányzati eseménykezelő központ egyidejű tájékoztatása mellett az NTG-hez csatlakozott szervezetet ideiglenes jelleggel kizárni, amennyiben az érintett szervezet felől érkező azonosított adatforgalom (pl.: DDOS támadás, adathalászat, stb.) az NTG-hez csatlakozott intézmények elektronikus információbiztonságát, illetve az NTG működését hátrányosan befolyásolhatja vagy veszélyeztetheti.

6.2. ideiglenes jelleggel kizárni azt a szervezetet – az érintett szervezet és a Nemzeti Elektronikus Információvédelmi Hatóság, illetve a kormányzati eseménykezelő központ egyidejű tájékoztatása mellett – amelyik más adathálózattal, vagy nyílt internettel összekapcsolja NTG végpontját, és ezzel a csatlakozott szervezetek illetve az NTG-re kapcsolódó hálózatok és szolgáltatások információ biztonságát, illetve működését veszélyezteti.