Iktatószám: 1/2019

Informatikai Biztonsági Szabályzat 2019.

Felülvizsgálva 2022. Ü hó

I. Fejezet

Általános Rendelkezések

Az Informatikai Biztonsági Szabályzat célja, hatálya

1. § Az Informatikai Biztonsági Szabályzat célja

A Fővárosi Önkormányzat Kútvölgyi Úti Idősek Otthona (a továbbiakban: Intézmény) magára nézve kötelezőnek ismeri el jelen szabályzat tartalmát.

Az Intézmény elkötelezett a természetes személyek személyes adatainak védelmében, kiemelten fontosnak tartja információs önrendelkezési jog tiszteletben tartását. Az Intézmény a személyes adatokat bizalmasan kezeli, és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy az Intézménynél a szervezeti egységek és munkatársaik egymás közötti és az Intézményhez nem tartozó külső szervekkel, személyekkel fenntartott kapcsolatokban biztosítható legyen:

a) az Intézmény informatikai rendszereinek (a továbbiakban: rendszerek) és a rendszerekben tárolt adatok megfelelő rendelkezésre állása;

b) az adatállományok formai és tartalmi helyességének, épségének megőrzése;

c) az adatok és információk bizalmassága, megfelelő védelme;

d) az Intézmény tevékenysége során keletkezett személyes adatok védelme;

e) a vagyon-, munka- és tűzvédelemre vonatkozó előírások betartása;

f) a számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő hátrányos következmények megszűntetése, illetve minimális mértékre való csökkentése;

g) az informatikai szoftver eszközökkel kapcsolatos jogbiztonság, jogtisztaság;

h) a jogszabályi szinten rögzített adatvédelmi és adatbiztonsági elvárásoknak való megfelelés.

A vázolt célok elérése érdekében a védelemnek működnie kell a rendszerek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül – a felszámolásukig. Az IBSZ alkalmazásánál figyelembe kell venni, hogy az Intézmény különböző szervezeti egységei használatában működő telekommunikációs és informatikai rendszerek tervezése, bevezetése, üzemeltetése és ellenőrzése vonatkozásában meghatározott feladatok elsősorban a törvényesség betartásával, másodsorban a védelem hiányából eredő lehetséges károk értékével legyenek arányosak.

2. § Az IBSZ hatálya

(1) Az IBSZ személyi hatálya kiterjed az Intézmény valamennyi közalkalmazotti jogviszonyban, továbbá munkaviszonyban foglalkoztatott munkatársára (a továbbiakban együtt: munkatársak). Az IBSZ személyi hatálya kiterjed továbbá minden személyre, aki az Intézmény informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül az Intézményhez kapcsolódó jogviszonyától. Más természetes személyeket az IBSZ csak a külön adatvédelmi megállapodásokban (pl. adatszolgáltatás, hozzáférés, titoktartás) rögzítettek szerint érint.

(2) Az IBSZ tárgyi hatálya kiterjed:

a) valamennyi (az Intézmény tulajdonában lévő, vagy általa bérelt) informatikai és telekommunikációs berendezésre, vagy az Intézmény használatában álló épületben található, leltári jelzéssel ellátott, továbbá az Intézmény megbízásából az Intézmény munkatársai számára harmadik személy által biztosított informatikai eszközre, beleértve a berendezések műszaki dokumentációját is;

b) az Intézmény eszközein működtetett rendszerprogramokra és a felhasználói programokra;

c) amennyiben az Intézmény működésére irányadó egyéb szabályzat eltérően nem rendelkezik:

ca) az informatikai folyamatot leíró valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentációk);

cb) az adathordozók tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is, kivéve;

cc) az adatok felhasználására;

cd) a védelmet élvező adatok teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól (bizonylatok, tablók, mágneses adathordozók, stb.) függetlenül;

ce) minden olyan adatkezelésre és adatfeldolgozásra, amely az Infotv. szerinti személyes, különleges, közérdekű, vagy közérdekből nyilvános adatra vonatkozik, és az adatkezelés, illetve adatfeldolgozás teljesen vagy részben automatizált eszközzel történik.

(3) Az IBSZ rendelkezéseit értelemszerűen alkalmazni kell minden olyan adatkezelésre, amelyet az Intézmény, mint adatkezelő szerv vezetőjének meghatalmazása alapján külső szervezet végez, valamint a beléptető rendszerben történő adatkezelésre is.

II. Fejezet

Az IBSZ-hez kötődő egyéb szabályozások

3. § Az IBSZ a jogszabályok előírásainak alkalmazásán alapul, és az információvédelemre vonatkozó jogszabályi szintű rendelkezésekkel – így különösen az Adatvédelmi kódexben és az Intézmény Adatvédelmi Szabályzatában felsorolt törvényekben és a végrehajtásukra kiadott jogszabályokban foglaltakkal – együtt értelmezendő:

4. § Az IBSZ-ben nem rendezett kérdésekben a fentiekben említett hatályos jogszabályok rendelkezéseit, továbbá az Intézmény egyéb belső szabályzataiban, így különösen a Szervezeti és Működési Szabályzatban, az Iratkezelési Szabályzatban, a Közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló Szabályzatban, a Tűzvédelmi Szabályzatban foglaltak az irányadók.

III. Fejezet

Értelmező rendelkezések

5. § Az IBSZ alkalmazása során:

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

b) adatállomány: az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok összessége;

c) adatátvitel: adatok informatikai rendszerek, rendszerelemek közti továbbítása;

d) adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni technikai, szervezési megoldások és eljárási szabályok összessége, az adatkezelésnek azon állapota, amelyben a fenyegetettséget jelentő kockázati tényezőket különböző műszaki, szervezési megoldások és intézkedések a lehető legkisebb mértékűre csökkentik;

e) adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

f) adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik;

g) adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

h) adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

i) adathordozó: bármely alakban, bármilyen eszköz felhasználásával és bármilyen eljárással előállított, adat tárolására alkalmas, továbbá adatot tartalmazó anyag;

j) adatvédelem: a személyes adatok kezelésének normatív szabályozása az érintett információs önrendelkezési jogának biztosítása és érvényesítése érdekében;

k) adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

l) alapszolgáltatások: azok az informatikai szolgáltatások, amelyek minden felhasználó számára rendelkezésre állnak;

m) alkalmazás: a szoftver és minden egyéb olyan számítógépes program, amelyet egy feladat vagy feladatkör végrehajtására terveztek;

n) authentikáció: az adatcsere során a kommunikációban résztvevő felek identitása megállapításának és ellenőrzésének folyamata;

o) *azonosító eszköz*: olyan eszköz, amely a felhasználó egyértelmű azonosítására szolgál (pl. mágneskártya, Proximity kártya;

p) *auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

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

r) *biztonsági esemény*: bármilyen olyan esemény, ami az érvényben lévő biztonsági szabályokat sérti, vagy a biztonsági szabályok sérülésének gyanúját vetik fel, így különösen az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, melynek hatására az informatikai rendszerben tárolt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült, vagy megsérülhet;

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

t) *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

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

v) *biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

w) *biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

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

y) *érintett:* bármely meghatározott, személyes adat alapján azonosított, vagy – közvetlenül vagy közvetve – azonosítható természetes személy;

z) *biztonsági rendszer*: az épületek betörés és vagyonvédelmi rendszere, valamint az ehhez kapcsolódó beléptető rendszerek;

IV. Fejezet

Az informatikai biztonsághoz kapcsolódó rendelkezések

6. § Az Intézmény működése szempontjából kritikus, kiemelt, normál és egyéb rendszerek

(1) Az Intézmény működése szempontjából kritikus az a rendszer, amely az Intézmény egészére kiterjed, vagy amely összefügg az Intézmény alaptevékenységével, vagy amely szemé-

lyes adatot tartalmaz. A kritikus rendszerek adatbiztonsági szempontból kiemelt védelmet igényelnek. E körbe tartoznak különösen az alábbi rendszerek:

a) bér- és munkaügyi rendszer;

b) gazdasági, ügyviteli rendszer;

c) iratkezeléssel összefüggő rendszerek;

d) támogatással, pályáztatással összefüggő rendszerek;

e) központi levelező kiszolgálók;

f) központi tárhely kiszolgálók;

g) intézményi authentikációs rendszerek.

(2) Az Intézmény szempontjából kiemelt rendszerek azok, melyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek. E körbe különösen az alábbi rendszerek tartoznak:

a) telekommunikációs rendszer és hálózat;

b) kommunikációs rendszerek;

c) technológiai rendszerek.

(3) Normál rendszerek a kritikus és kiemelt rendszerek körébe nem sorolt, de az Intézmény napi működése szempontjából kritikus, továbbá az Intézmény egészére nem, csak egyes részeire kiterjedő olyan rendszerek, amelyek használatához szükséges a személyes authentikáció.

(4) A kritikus, kiemelt és normál rendszerek körébe nem sorolt rendszerek.

7. § Kockázatkezelés

(1) Minden kritikus rendszer és kiemelt rendszer besorolású szolgáltató rendszer esetében rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának az Intézmény működőképességére tett hatásait tartalmazza. Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérülésből származó hatásokat. A kockázatelemzési dokumentum előállítása és karbantartása a szolgáltatás üzemeltetőjének a feladata. Az elektronikus információs rendszerek kockázatait az Ibtv. végrehajtási rendelete, a 41/2015. (VII. 15.) BM rendelet által meghatározott követelményrendszer szerint is értékelni kell.

(2) Kritikus rendszer és kiemelt rendszer üzemeltetése az Intézmény működési területein kizárólag az intézményvezető engedélyével, míg normál rendszer és egyéb rendszer üzemeltetése az Intézmény területén a gazdasági vezető engedélyével történhet.

V. Fejezet

Infrastruktúrához kapcsolódó védelmi intézkedések

8. § (1) Az Intézmény épületeiben portaszolgálat működik.

(2) Az Intézmény a használt épületekben a helyiségek a védelem szempontjából naz alábbiak:

a) Pénztárhelyiség, kapcsolószekrények (kiemelt védelem)

b) Raktárak, szerviz/kiszolgáló helyiségek területe (fokozott védelem)

c) egyéb helyiségek, irodák, folyosók (alap védelem)

(3) Az Intézménynél a munkatársak belépéskor történő azonosítása a portaszolgálat feladata. A fokozott és kiemelt védelemmel ellátott biztonsági zónákba csak az arra jogosult személyek kapnak belépési jogosultságot. A kiemelt védelemmel ellátott helyiségekbe a belépési jogosultsággal rendelkező munkatársak léphetnek be

VI. Fejezet

Hardverekre és szoftverekre vonatkozó előírások

10. § (1) Az Intézmény a *központi rendszer*ekhez védelmet biztosít. Minden esetben, amikor a szerverhelyiségben, illetve vele, egyenrangú védelemmel rendelkező más területen szerverek és kommunikációs eszközök telepítése történik, biztosítani kell ezen eszközök biztonságos elkülönítését és védelmét (pl. szerver szoba és operátori szoba kialakítással).

A szervereket és a kommunikációs eszközöket (router, switch), azok fizikai védelme céljából, erre a célra kialakított jól szellőző, zárható szekrényben elzárva kell üzemeltetni.

A központi rendszer elemei telepítésének, áttelepítésének végrehajtása minden esetben az gazdasági vezető/műszaki vezető/informatikus feladata és felelőssége. Szerver vagy kommunikációs eszköz nem az IBSZ által előírt körülmények közötti elhelyezésére csak a gazdasági vezető előzetes és egyedi engedélye mellett van lehetőség és csak átmeneti jelleggel. A központi rendszerek telepítésénél a gazdasági vezetőnek/műszaki vezető/informatikus minden esetben kiemelten kell gondoskodni a berendezések biztonságáról, az illetéktelen hozzáférés megelőzéséről, megakadályozásáról. A központi rendszerekhez sem a rendszereket szállítók sem a rendszert fejlesztők nem rendelkezhetnek közvetlen hozzáférési jogosultsággal. Minden egyes külső beavatkozás (verzió-frissítés, programhiba javítás, egyedi fejlesztés stb.) során dokumentálni kell a program-változásokat, az elvégzett ellenőrzéseket, teszteléseket.

A központi rendszerekhez tartozó helyi hálózat megbízhatóságának növelésére, annak túlterhelését, hálózatrészek kiesését megelőző, a helyi adottságoknak megfelelően kiválasztott rendszertechnikai megoldásokat (redundáns átviteli utak, illetve aktív elemek, dinamikus átkonfigurálás, osztott hálózatvezérlés stb.) kell alkalmazni.

A számítástechnikai eszköz telepítésének részét képezi az eszköz verifikálása (ellenőrzése). A verifikálás eredményét, azaz hogy az eszköz a meghatározott biztonsági követelményeknek eleget tesz, azt a gazdasági vezető/műszaki vezető/informatikus köteles írásban rögzíteni.

(2) Munkaállomások, laptopok telepítése, konfigurációkezelése során az alábbiakat kell figyelembe venni:

a) Minden munkaállomás telepítést, módosítást, cserét az igénylő kezdeményez az alkalmazott eljárásrend szerint.

b) A munkaállomásokat csak a feladat ellátásához szükséges beállításokkal és programokkal szabad telepíteni.

c) A munkaállomások elhelyezésénél (fizikai telepítés) minden esetben kiemelten kell gondoskodni a berendezések biztonságáról, az illetéktelen hozzáférés megelőzéséről, megakadályozásáról. Azon irodahelyiségeket, ahol munkaállomás működik tilos felügyelet nélkül hagyni, ha a helyiségben senki sem tartózkodik, azt be kell zárni.

d) A munkaállomáson egyedi hozzáférést kell biztosítani, ezáltal lehetővé téve, hogy a munkaállomást csak az arra jogosult Felhasználók használhassák.

(3) Az Intézmény biztosítja az informatikai rendszerének egészére kiterjedő rendszeres és folyamatos vírusvédelmet. Vírusellenőrzés történik a helyi hálózaton, a levelező szerveren,

valamint az összes munkaállomáson. Az gazdasági vezető/műszaki vezető/informatikus által megbízott személy gondoskodik arról, hogy a vírusellenőrző programnak mindig a legújabb verziója működjön. A frissítéseknek maximum 1 munkanapon belül meg kell történniük. Csak jogtiszta és megfelelő dokumentációval ellátott vírusellenőrző program használata megengedett. A vírusellenőrző programot csak speciális esetekben, csak a gazdasági vezető/műszaki vezető/informatikus utasítására lehet kikapcsolni. A rendszergazda kötelessége, hogy a vírusvédelmet a lehető legrövidebb időn belül visszakapcsolja. A vírusirtó leállítását és újraindítását dokumentálni kell. A felhasználók a vírusvédelmet semmilyen körülmények között sem kapcsolhatják ki. A hatékony vírusvédelem érdekében az Intézmény munkatársaihoz kívülről érkező leveleken kiterjesztés és tartalom szerinti szűrést kell végezni, és a vírus gyanús leveleket azonnal karanténba kell helyezni.

(4) Amennyiben a vírusellenőrzések ellenére a felhasználók vírusra utaló hibás, vagy furcsa működést tapasztalnak, a vírusfertőzés gyanújáról azonnal értesíteni kell a gazdasági vezetőt/műszaki vezetőt/informatikust. A felhasználó köteles haladéktalanul jelenteni, ha rosszindulatú alkalmazás jelenlétének gyanúját észleli az informatikai eszközön. Rosszindulatú alkalmazás jelenlétére utaló jelek különösen:

a) rosszindulatú alkalmazás elleni védelemről gondoskodó alkalmazás névvel azonosított rosszindulatú alkalmazást jelez;

b) fájl másolása esetén a forrásfájl és a célfájl mérete, neve eltérő;

c) szokatlan és váratlan képernyő tevékenység;

d) szokatlan alkalmazás-tevékenység: felhasználói beavatkozás nélkül elinduló alkalmazások, a megszokottól eltérően viselkedő alkalmazások, elérhetetlen funkciók, stb.;

e) jelentősen lassult működés, amely többszöri újraindítás során sem javul.

(5) Külső adathordozó használata előtt az adathordozó adatállományát a rosszindulatú alkalmazás elleni védelemről gondoskodó alkalmazás használatával ellenőrizni kell. A vírusdetektálás (vagy vírusgyanú felmerülése) és a víruseltávolítás biztonsági eseménynek számít, ezért minden vírusdetektálást és víruseltávolítást haladéktalanul jelenteni kell a gazdasági vezető/műszaki vezető/informatikus felé. Az ilyen eseményt ki kell vizsgálni és dokumentálni. Az gazdasági vezető/műszaki vezető/informatikus időszakosan ellenőrizni köteles, hogy az aktuálisan használt vírusellenőrző program megegyezik a kiadott legfrissebb változattal. A biztonsági kockázatot jelentő elektronikus küldemények kezelése során az Iratkezelési Szabályzat rendelkezéseit is figyelembe kell venni.

(6) Az Intézménybe új rendszer fejlesztésével, létező rendszerek továbbfejlesztésével, az új rendszerek, verziók bevezetésével és szükséges dokumentációival kapcsolatos biztonsági elvárásokat az Adatvédelmi kódex tartalmazza. A követelményjegyzéket az Intézmény minden rendszerfejlesztés, rendszerbevezetés tartalmú pályázatának, szerződésének mellékleteként csatolni kell, a benne foglaltakat a szállítóktól meg kell követelni.

Külső és belső ellenőrzési eszközökkel ellenőrizni kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket Valamennyi rendszer vagy rendszerelem, hardver és szoftver beszerzése során meg kell határozni és szerződéses követelményként elő kell írni:

a) a funkcionális biztonsági követelményeket;

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

c) a biztonsággal kapcsolatos dokumentációs követelményeket;

d) a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;

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

f) az elfogadási kritériumokat.

A rendszer fejlesztések során a rendszer valamennyi életciklusában értékelni és érvényesíteni kell a biztonsági követelményeket. Meg kell határozni a rendszerhez kapcsolódó információbiztonsági szerepköröket és felelősségeket.

A rendszer életciklus szakaszokat a következők szerint kell meghatározni:

a) követelmény meghatározás;

b) fejlesztés vagy beszerzés;

c) megvalósítás vagy értékelés;

d) üzemeltetés és fenntartás;

e) kivonás (archiválás, megsemmisítés).

(7) Az elektronikus információs rendszerek beszerzése és fejlesztése során meg kell követelni a rendszer adminisztrátori és fejlesztői dokumentációjának az elkészítését, melyeknek tartalmazniuk kell rendszer biztonsági vonatkozásait, a biztonságos konfigurálását, telepítését és üzemeltetését, a biztonsági funkciók hatékony alkalmazását és fenntartását, ismert sérülékenységeket, továbbá a felhasználó által elérhető biztonsági funkciókat és a felhasználó kötelezettségeit a biztonság fenntartásához;

Az Intézmény a rendszer karbantartások és az azokhoz kapcsolódó ellenőrzések elvégzése érdekében rendszer-karbantartási eljárásokat alakít ki. A karbantartási tevékenységekről nyilvántartást vezet. A karbantartások tervezése és végrehajtása során:

a) a gyártói vagy a forgalmazó specifikációknak megfelelően, továbbá a szervezeti igények szerint a karbantartásokat és javításokat ütemezetten hajtja végre;

b) dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket;

c) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;

d) külső karbantartó személyzet esetén minden esetben ellenőrizni kell karbantartást végzők, szervezetek vagy személyek jogosultságát a munka elvégzésére;

e) a gazdasági vezetőnek vagy az általa meghatalmazott felelős munkatársak jóváhagyása szükséges az elektronikus információs rendszer vagy a rendszerelemek Intézmény létesítményeiből történő kiszállításhoz;

f) gondoskodik arról, hogy az elszállítás előtt minden adat és információ – mentést követően –a berendezésről törlésre kerüljön;

g) a javítási tevékenységek után ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;

h) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

(8) A karbantartási terveket és eljárásokat évente felül kell vizsgálni és szükség szerint aktualizálni.

VII. Fejezet

Az adathordozók kezelése és biztonsága

11. § Az adatok sérülésének elkerülésére és a működésfolytonosság fenntartás érdekében üzemeltetési eljárásokat kell létrehozni az elektronikus dokumentumokhoz, számítógép médiumokhoz, adathordozókhoz történő jogosulatlan hozzáférés, módosítás, ellopás megakadályozása érdekében. A védelem szabályozási, logikai és fizikai eljárásokat tartalmaz.

12. § Az eltávolítható adathordozók kezelése:

A hordozható adathordozók – más terminológia szerint eltávolítható adathordozók – jellegükből adódóan jelentős információbiztonsági kockázatot hordoznak.

Az eltávolítható adathordozók közé tartoznak az adatkazetták, CD-k, DVD-k, külső merevlemezek, pendrive-ok, de ebbe a kategóriába kell sorolni hozzáférhetőségük és felépítésük miatt a mobiltelefonok és fényképezőgépek memóriáját is. (Általában használatos még az „USB mass storage" elnevezés is.)

A legnagyobb veszélyt az eltávolítható adathordozók jogosulatlan használata jelenti. Az Intézmény hálózatához ilyen eszközt kapcsolva fennáll a rosszindulatú kódok (vírusok) bejutásának veszélye, másrészről pedig fennáll az adatok jogosulatlan elvitelének veszélye, ezért a dolgozók saját **eltávolítható adathordozóikat külön feljogosítás nélkül a hálózathoz nem csatlakoztathatják!**

13. § (1) Az eltávolítható adathordozókkal kapcsolatos irányelvek:

a) bizalmas információ csak titkosítva írható fel rájuk;

b) biztosítani kell hardver titkosítással ellátott pendrive-okat azon munkatársak számára, akiknek munkájához indokolt;

c) a titkosítatlan optikai adathordozókat, amennyiben már nem szükségesek, helyreállíthatatlanul fizikailag meg kell semmisíteni;

d) a megőrzendő adatok esetében, figyelembe kell venni az eszköz várható élettartamát és ennek megfelelően időközönként át kell másolni az adatokat vagy több helyen kell azokat tárolni.

14. § (1) Adathordozók újrahasznosítása és selejtezése

Az adatok kiszivárgásának megakadályozás érdekében az alábbi utasításokat kell követni:

a) A már szükségtelenné vált adatot tartalmazó, de újrafelhasználható adathordozókról – tipikusan munkaállomások, laptopok merevlemezei, új felhasználóhoz történő kiadásuk előtt – elegendő az adatokat szokásos formázási vagy törlési eljárással törölni, majd az eszközt újra használatba lehet venni. Ez kizárólag a szervezeten belül történő újrafelhasználás esetén érvényes.

b) A használaton kívüli adathordozókat osztályozni kell aszerint, hogy tartalmaz-e érzékeny adatot. Amennyiben ez nem megállapítható, akkor az adathordozót úgy kell kezelni, mint ami érzékeny adatot tartalmaz.

c) Az érzékeny adatokat tartalmazó mágneses adathordozókat (merevlemezeket) lemágnesezéssel vagy speciális felülírással lehet törölni.

d) Azokat az adathordozókat, amelyek már további használatra nem alkalmasak, selejtezni kell. A selejtezésre szánt adathordozókról jegyzőkönyvet kell felvenni, s az adatmegsemmisítést is bizottságilag jegyzőkönyvezni kell.

e) Valamennyi adathordozó típus esetén alkalmazható a speciális, adatmegsemmisítéssel foglalkozó cégek szolgáltatása, amelyek bezúzással, vagy égetéssel, jegyzőkönyvezés mellett végzik a megsemmisítést.

A nem elektronikus – jellemzően papír alapú – adathordozók esetében is hasonlóan kell eljárni, a használatból kivont adathordozókat első sorban fizikailag kell megsemmisíteni.

15. § (1) Az adathordozók tárolása és védelme:

a) Az adathordozókat a rajtuk lévő adatok érzékenységének megfelelően, védeni kell, használaton kívül el kell zárni.

b) Adathordozó (adat) az Intézmény területéről csak az Intézmény vezető engedélyével kerülhet ki, ez vonatkozik az adathordozókon történő kivitelre, vagy az egyéb, elektronikus úton történő továbbításra, mint az Internet vagy a (mobil)telefonos adattovábbítás.

c) A központi infrastruktúrán (kiszolgálók, csoportkönyvtárak, fájl szerverek stb.) kívül például felhasználói munkaállomásokon, laptopokon csak olyan adatot szabad tárolni, melyek sérülése, elvesztése vagy illetéktelenek kezébe történő kerülése nem okozhat az Intézmény számára kárt vagy bizalomvesztést. Az ilyen adatok nem kerülnek központi mentésre, ezért a mentési igényt minden esetben az Gazdasági igazgató felé kell jelezni.

d) A személyi használatra kiadott laptopokon bizalmas információ csak titkosítva szabad tárolni.

VIII. Fejezet

Dokumentációkhoz kapcsolódó védelmi intézkedések

16. § (1) Minden nyilvántartott szoftverhez nyilván kell tartani a szoftver dokumentációját, ami magába foglalja legalább az alábbiakat:

a) felépítésének, funkcióinak és adatkapcsolatainak felső szintű leírását, valamint alapvető jellemzőit (mérete, nyelve, működési környezet, készítőjét), leírását;

b) felhasználói és üzemeltetői kézikönyveket, különösképpen a felhasználói jogosultság rendszer leírását, továbbá a felhasználó kötelezettségeit a biztonság fenntartásához;

c) a rendszer telepítőkészletét, telepítési segédleteit;

d) a tesztelést igazoló, valamint az üzemeltetésre átvétel jegyzőkönyveit;

e) az üzemi, konfigurációs beállítások leírását;

f) a rendszert üzemeltetésével, támogatásával kapcsolatos partneri megállapodásokat (pl.: licencek, support szerződések, elérhetőségek);

g) a rendszer biztonsági vonatkozásait, az ismert sérülékenységeket, biztonsági funkciók hatékony alkalmazását és fenntartását.

(2) A felsorolt dokumentumok őrzése a titkárság/ gazdasági vezető/műszaki vezető/informatikus feladata. A rendszerleírási és rendszerprogram dokumentációinak első példányát a központi irattárban kell tárolni elektronikus formában. A leírások és dokumentációk másodpéldányát papíron (és lehetőség szerint elektronikus formában is) tűzbiztos lemezszekrényben, kell tárolni. A dokumentációkat minden esetben úgy kell elhelyezni, hogy azok a tárolás közben ne sérüljenek vagy károsodjanak.

Gondoskodni kell arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;

Gondoskodni kell a dokumentációknak az érintett szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

(3) A rendszerleírások és rendszerprogram dokumentációinak frissítését minden olyan esetben, amikor a rendszeren változtatás (rendszerkonfiguráció változtatás, javítás, verzióváltás, stb.) az üzembe állítás (üzemeltetésre átadás) előtt frissíteni kell. A dokumentációk naprakészségért a gazdasági vezető/műszaki vezető/informatikus felelős. A rendszerleírásokról és rendszerprogram dokumentációkról űrlapon kell pontos nyilvántartást vezetni, a verziószámoknak és a telepítés időpontjainak a feltüntetésével. A nyilvántartásnak biztosítania kell, hogy legalább 1 évre visszamenőleg meghatározható legyen minden, az egyes rendszerekkel kapcsolatos változás ideje, oka, mibenléte. A nyilvántartás vezetése és annak folyamatos aktualizálása a gazdasági vezető/műszaki vezető/informatikus feladata.

(4) A felhasználói dokumentációk folyamatos rendelkezésre állása megköveteli, hogy a dokumentumokat gyorsan és egyszerűen el lehessen érni. A felhasználói dokumentációkat javasolt elektronikusan, nyilvános mappában, vagy intraneten tárolni.

IX. Fejezet

Elektronikus kommunikációhoz kapcsolódó védelmi intézkedések

17. § Általános rendelkezések

(1) E-mail használattal kapcsolatos előírások

Az e-mail használatával kapcsolatos, jelen pont alatti előírásokat akkor kell alkalmazni, ha az Intézmény működésére irányadó egyéb szabályzat, így különösen az Iratkezelési Szabályzat másként nem rendelkezik. Az elektronikus levelezés célja a gyors ügyintézés és a papír alapú dokumentumok mennyiségének csökkentése. Az Intézmény minden munkatársával szemben elvárás az elektronikus levelezéssel kapcsolatban a körültekintő és etikus viselkedés. Az Intézmény munkatársaira az alábbi, az elektronikus levelező rendszerre vonatkozó jogok és kötelezettségek vonatkoznak:

a) a belső elektronikus levelező rendszerben továbbított üzenet, levél, vagy csatolt fájl egyenértékű az üzenet, levél, vagy csatolt fájl személyes, papír alapon történő átadásával;

b) az elektronikus levelező rendszerből kifelé továbbított üzenet nem vonatkozhat kötelezettség vállalásra;

c) az elektronikus levelező rendszerből kifelé továbbított bizalmasan kezelendő üzenet csak titkosítva küldhető;

d) az elektronikus levelező rendszerből kifelé továbbított levélben és üzenetben minden esetben biztosítani kell az Intézmény jó hírét;

e) elektronikus levelezéskor az elektronikus levelezési címet csak az arra jogosult személy használhatja, más nevében elektronikus levél küldése nem engedélyezett;

f) az elektronikus levelező rendszer használata során minimálisra kell csökkenteni annak személyes célokra történő használatát, az elektronikus levelező rendszerrel személyes üzleti tevékenység nem végezhető;

g) a téves címzés miatt megkapott levelet bizalmasan kell kezelni, és azt haladéktalanul az eredeti címzettjének vagy a feladójának kell továbbítani;

(2) Vezeték nélküli hozzáférés

Az Intézmény a mobil eszközökkel rendelkező felhasználói számára, egyedi engedélyezési eljárás után, vezeték nélküli (WiFi) hozzáférési lehetőséget biztosíthat elektronikus információs rendszereihez.

A vezeték nélküli hálózat létesítése és üzemeltetése során az alábbi feltételeknek kell teljesülniük:

a) A vezeték nélküli hozzáférést titkosítással és a felhasználók, vagy eszközök hitelesítésével kell védeni,

b) A vezeték nélküli hálózat konfigurálását a rendszergazdák csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül végezhetik.

c) A vezeték nélküli hálózat üzemeltetése során megfelelő karakterisztikájú és teljesítményszintű antennák, vagy egyéb technikákat alkalmazásával gondoskodni kell arról, hogy a szervezet fizikai határain kívülről a jelek észlelésének a valószínűsége minimális legyen.

18. § Kommunikáció biztonságának szabályozása

(1) Behatolás védelmi szabályok, és tűzfalak:

a) Az Intézmény a Központi rendszereit tűzfallal vagy azzal egyenértékű tűzfal jellegű berendezéssel (továbbiakban: Tűzfal) köteles védenie annak megakadályozására, hogy kívülről illetéktelen személy a rendszerbe behatolhasson. Az ilyen védelmi feladatot ellátó berendezést a Központi rendszerek részének kell tekinteni.

b) A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.

c) Az Intézmény hálózatáról szigorúan tilos bármilyen, a tűzfalat megkerülő kapcsolatot létesíteni nyilvános hálózatokkal (pl.: Internetet modemen keresztül használni).

d) Nem nyilvános hálózatokat csak ellenőrzött kapcsolaton keresztül szabad használni.

e) Az alkalmazott tűzfal auditáltatását, annak üzembe helyezését követően, külső szakértővel el kell végeztetni.

f) Az alkalmazott tűzfalon változtatást csak a hálózati eszközök Rendszergazdája végezhet, ha azt a gazdasági vezető/műszaki vezető/informatikus előzetesen engedélyezte.

g) Az alkalmazott tűzfal berendezésen végrehajtott változásokat a Rendszergazdának dokumentálnia kell (ki és mikor végezte a beavatkozást, mit módosított), és

erről a gazdasági vezetőt/műszaki vezetőt/informatikust haladéktalanul értesíteni köteles.

h) Az alkalmazott tűzfal működőképes konfigurációjáról olyan biztonsági másolatot kell készíteni, amelynek segítségével a korábbi működő állapot - szükség esetén - gyorsan előállítható. A biztonsági másolatot a normál mentésekkel együtt tűzbiztos széfben kell eltárolni.

i) A központi rendszereken végzett bármilyen olyan beállítás, amihez rendszergazdai jogosultság szükséges, csak az Intézmény területén végezhető.

j) Ha a központi rendszerekhez - rendkívüli esetben - távoli helyről válik szükségessé rendszergazdai beavatkozás, akkor ez - a megfelelő óvintézkedések (egyszeri jelszó, hívás-visszahívás eljárás stb.) megtétele mellett végezhető el.

k) Biztosítani kell, hogy az Intézmény Informatikai rendszerének bármely elemén kizárólag csak az arra felhatalmazott rendszergazda végezhessen rendszergazdai jogosultsághoz kötött módosításokat. Felhasználók még átmenetileg sem kaphatnak ilyen jogosultságot.

l) Megtörtént, vagy folyamatban levő biztonsági incidens észlelésekor a felhasználó haladéktalanul köteles értesíteni a gazdasági vezetőt/műszaki vezetőt/informatikust. A felhasználó nem kísérelheti meg a támadó felderítését, nem tehet ellenlépéseket, kivéve, ha erre kifejezett utasítást kap

(2) Titkosítás, elektronikus aláírás:

Az Intézmény nem tervezi PKI eszközök használatba vételét, és jelenleg nem használ semmilyen titkosítási, vagy elektronikus aláírási megoldást..

X. Fejezet

Személyekhez kapcsolódó védelmi intézkedések, azonosítás és hitelesítés

19. § Általános előírások

Az Intézmény biztosítja, hogy minden munkatársa megfelelő hozzáféréssel rendelkezzen a munkaköréhez szükséges informatikai alapszolgáltatásokhoz. Az Intézmény minden munkatársa számára biztosítja a munkakör ellátásához szükséges Alkalmazói szoftverek, illetve az Alkalmazói szoftverek meghatározott részeinek rendeltetésszerű használatát. A jogosultságok felhasználókhoz kötődnek. A felhasználó számára biztosított jogosultság alapján az adatokon végzett minden tevékenységgel és az adatok felhasználásával kapcsolatos minden felelősség a felhasználót terheli. Azon Alkalmazói szoftverek esetében, ahol a szolgáltató egy intézmény részére csak egy (általában az intézmény vezetőjéhez kapcsolt) hozzáférési jogosultságot biztosít, ott a jogosultság továbbadásával érintett felhasználót terhel minden felelősség az adatokon végzett minden tevékenységgel és az adatok felhasználásával kapcsolatban. Az Intézmény gondoskodik arról, hogy az informatikai rendszerében tárolt adatokhoz illetéktelen ne férjen hozzá, adatolvasást, adatmegsemmisítést, adathamisítást ne tudjon végrehajtani.

20. § A felhasználó azonosítása és hitelesítése, hozzáférés szabályozás

Minden felhasználó saját, kizárólagos használatú egyedi azonosítóval (User ID) rendelkezik, mely használatával, magát jelszavával hitelesítve, hozzáfér a rendszer erőforrásokhoz.

Az egyedi azonosító alkalmas arra, hogy a végzett tevékenységek nyomon követhetőek legyenek, s hozzájuk egyéni felelősség legyen rendelhető.

A felhasználói azonosító nem utalhat a szerepkör esetleges privilégiumára (például rendszergazda vagy üzemeltető stb.)

Csoportos felhasználói azonosító nem engedélyezett – kivéve azokban az esetekben, ahol egyéb nyilvántartás alapján megadható, hogy ki használja az adott fiókot. Szerződött partnerek, külső támogatók (harmadik fél) valamennyi, az Intézmény rendszereihez hozzáférési jogosultsággal rendelkező munkatársának saját azonosítót kell igényelnie, amelynek kezelése a belső alkalmazotti azonosítókkal azonos módon történik.

Amennyiben fokozott biztonságú hitelesítés a követelmény, akkor a jelszó mellett további hitelesítési eszközök használatát, mint kriptográfiai eszközök, memóriakártya, tokenek vagy biometrikus azonosítás kell bevezetni

Az azonosítók ismételt felhasználása – mivel személyhez kötött, egyedi azonosítókról van szó – nem engedélyezett, kivéve abban az esetben, amennyiben a korábban kilépett munkatárssal létesít újra munkaviszonyt az Intézmény.

Három hónapos inaktivitás után a nem használt azonosítókat le kell tiltani.

21. § A hitelesítésre szolgáló eszközök kezelése:

a) gondoskodni kell róla, hogy a hitelesítésre szolgáló eszközök átadásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultsága ellenőrzésre kerüljön;

b) meg kell határozni a hitelesítésre szolgáló eszköz kezdeti tartalmát;

c) biztosítani kell a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

d) dokumentálni kell a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;

e) a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét meg kell változtatni az elektronikus információs rendszer telepítése során;

f) meg kell határozni a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;

g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként meg kell változtatni vagy frissíteni a hitelesítésre szolgáló eszközöket;

h) meg kell óvni a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;

i) a hitelesítésre szolgáló eszközök felhasználóinak kötelességük, hogy védjék eszközeik bizalmasságát, sértetlenségét;

j) az érintett fiókok megváltoztatásakor le kell cserélni a hitelesítésre szolgáló eszközt.

k) az elektronikus információs rendszer a hitelesítési folyamat során biztosítson fedett visszacsatolást, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

22. § 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.

XI. Fejezet

Személyi biztonság

23. § (1) A felhasználók tevékenységének ellenőrzése és szabályozása érdekében az Intézmény:

a) szabályzataiban rögzíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő munkatársakkal, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;

b) az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;

c) a követelmények változásáról az érintett munkatársakat értesíti.

(2) A felhasználók kötelezettségeként előírt védelmi intézkedések

Az Intézmény informatikai eszközein és hálózati meghajtóin kizárólag a felhasználó munkakörével és munkájával kapcsolatos adatok tárolhatók. A felhasználó saját, munkájával összefüggésbe nem hozható adatait az Intézmény által ezzel megbízott személy előzetes felszólítás nélkül törölheti. A felhasználó felel az általa használt informatikai eszközökön tárolt adatok védelméért, így különösen köteles:

a) a bizalmasan kezelendő és belső használatú információkat hordozható eszközökön titkosítva tárolni;

b) tartózkodni a bizalmasan kezelendő és belső használatú információk kódolatlan külső hálózaton történő küldésétől;

c) tartózkodni a jelszavak titkosítás nélküli tárolásától;

d) a mobil eszközök valamennyi biztonsági szolgáltatását használni;

e) az asztali számítógépet és a hordozható számítógépet jelszóval védeni;

f) a felügyelet nélkül hagyott asztali számítógépet és a hordozható számítógépet zárolni.

A felhasználó adatkezelését, ideértve különösen az adatok másolását, áthelyezését, továbbítását, fel- és letöltését az Intézmény adatbiztonsága érdekében naplófájlban rögzítheti és tárolhatja.

(3) Az Intézmény informatikai rendszereihez az alábbi hozzáférési csoportokat határozza meg:

a) Az alapszolgáltatás hozzáférés az Intézmény által meghatározott irodarendszerekhez való hozzáférést biztosítja, ami minden felhasználói munkaállomáson rendelkezésre áll.

b) Az alkalmazói szoftver hozzáférés az alkalmazói szoftver használatát biztosítja, ami a felhasználói terület erre jogosult munkatársának munkaállomásán rendelkezésre áll.

c) Speciális IT szolgáltatás hozzáférés a speciális informatikai szolgáltatások (pl. Internet, Laptop használat) igénybe vételét biztosítja.

d) A rendszergazda hozzáférés a Rendszerszoftverekhez (operációs rendszerek) és a rétegszoftverekhez (adatbázis-kezelők) való hozzáférést biztosítja, ilyen jogosultsággal a kinevezett rendszergazdák rendelkeznek.

e) A rendszerüzemeltető hozzáférés a Felhasználók alkalmazói szoftverbeli hozzáférési jogosultság beállítását teszi lehetővé, ilyen jogosultsággal a kinevezett rendszerüzemeltetők rendelkeznek.

(4) Jogosultságok kiadása

(5) Jogosultságok módosítása, letiltása

Egy munkatárs jogosultságainak bővítése, szűkítése az illetékes egység vezető kezdeményezésére, az Intézmény vezető engedélyével történhet. Meg kell különböztetni, hogy a bővítés vagy szűkítés csak egy adott munkatársat, vagy minden, adott munkakörben dolgozó munkatársat érint-e, és szükség esetén a munkakörökhöz tartozó jogosultsági listát is módosítani kell. A kilépett munkatárs személyes dokumentumainak (pl. levelezés, személyes könyvtár tartalma) CD-re másolásáról a kilépés napjáig a felhasználó kérésére az Intézet gondoskodik, és biztosítja, hogy csak a személyes dokumentumok kerülhessenek másolásra. A Felhasználók és Rendszergazdák jogosultságainak megváltoztatását előíró, az Gazdasági igazgató jóváhagyását tartalmazó leveleket, dokumentumokat iktatni kell.

24. § Információbiztonsági tudatosság és képzés

(1) Képzés munkába álláskor

Annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést kell nyújtani az elektronikus információs rendszer felhasználói számára. Az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében kötelező.

Először munkába álláskor, illetve a szerepkör átvételét megelőzően kell megtartani az információbiztonsági / adatvédelmi oktatást.

Az információbiztonsági oktatásnak a munkakör igényei szerint:

a) alkalmazkodnia kell az alkalmazott által betöltött feladatkörhöz,

b) tartalmaznia kell az ismert fenyegetésekre történő felkészülést,

c) ismertetnie kell az információbiztonság belső szervezetét

d) ismertetnie kell az információbiztonsági fenyegetések felismerésének módját és a szükséges intézkedéseket, eszkalációt.

(2) Rendszeres információbiztonsági / adatvédelmi frissítő képzés

Éves rendszerességgel meg kell ismételni az információbiztonsági tudatosságot frissítő képzést, amelyen minden, számítógépet használó munkatársnak részt kell vennie. Az éves frissítő képzések során:

a) ellenőrizni és frissíteni kell az alapvető információbiztonsági tudatossággal kapcsolatos ismereteket

b) tájékoztatni kell a munkatársakat az újabb fenyegetésekről és az azok elleni védekezésről,

c) ismertetni kell az információ-feldolgozó eszközök helyes használatára vonatkozó tudnivalókat és változásokat,

d) tájékoztatást kell adni a szoftverjogi követelmények alapjairól,

e) frissíteni kell az információbiztonsági incidensek kezelésével kapcsolatos tudnivalókat.

A képzések megtörténtét dokumentálni kell.

25. § (1) Eljárás a jogviszony megszüntetése esetén

Egy munkatárs kilépése esetén gondoskodni kell arról, hogy az elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátása továbbra is biztosított legyen, ezt a munkaköri feladatok és dokumentumok átadásátvételi folyamata biztosítja. A kilépő munkatárs munkahelyi vezetője jelöli ki az átvevő személyét.

Meg kell előzni azt, hogy a jogviszonyt megszüntető munkatárs esetlegesen az elektronikus információs rendszert, illetve abban tárolt adatokat bármilyen formában jogosulatlanul törölje, módosítsa vagy másolatot készítsen azokról, vagy más módon megsérthesse az elektronikus információbiztonsági szabályokat. Tájékoztatni kell kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről.

A kilépés során, a jogviszony megszűnését megelőzően gondoskodni kell a kilépő:

a) elektronikus információs rendszerekhez történő hozzáférési jogosultságainak megszüntetéséről;

b) egyéni hitelesítő eszközeinek visszavételéről vagy megszüntetéséről;

c) az Intézmény tulajdonában álló informatikai eszközök visszavételéről A Intézmény megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz, beleértve a kilépő elektronikus levelezését és tárolt dokumentumait.

Szükség esetén tájékoztatja a jogviszony megszűnéséről a kilépő munkatárssal munkakapcsolatban lévő belső és külső munkatársakat.

(2) Fegyelmi intézkedések

A Intézmény fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Amennyiben az elektronikus információbiztonsági szabályokat nem az Intézmény személyi állományába tartozó személy sérti meg, akkor érvényesíteni kell a vonatkozó szerződésben meghatározott következményeket és meg kell tenni a szükséges jogi lépéseket.

XII. Fejezet

Mentés, archiválás

26. § (1) A hálózati meghajtókon tárolt adatok biztonsága érdekében az adatokról az Intézmény rendszeresen mentést végez, és/vagy redundáns merevlemezekkel működő szervereket üzemeltet. Meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

a) meg kell határozni minden elektronikus információs rendszerre vonatkozóan a mentések szükséges gyakoriságát, a mentendő adatok körét;

b) a mentésekre vonatkozó igényeket összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal (RPO, RTO) a szakmai területekkel egyeztetve kell kialakítani.

(2) Az Intézmény meghatározott gyakorisággal elmenti az elektronikus információs rendszerek dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

a) megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen;

b) a legfontosabb adatokról a szakmai igények szerinti gyakorisággal és részletezettséggel archiválást végez.

(3) A mentési és archiválási adathordozókat azonosító sorszámmal látja el és azokról nyilvántartást vezet.

Az archiválásokat és mentéseket tartalmazó adathordozókon jól láthatóan és azonosíthatóan fel kell tüntetni az adathordozó azonosítóját. A mentések és archiválások típusát és idejét az eszközöktől függő módon, manuálisan vagy elektronikusan nyilván kell tartani.

Az archiválásokat és mentéseket tartalmazó adathordozókat a hálózati meghajtóktól és szerverektől elkülönített épületben, zárt helyiségben vagy szekrényben kell őrizni. Rendszeresen ellenőrizni kell a mentések és archiválások helyreállíthatóságát, tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében.

(4) Külső elérésekhez kapcsolódó védelmi intézkedések

Az Intézmény hálózatát elérhetővé kell tenni külső telephelyekről, hogy az itt alkalmazott szoftvereket a fejlesztők, adminisztrátorok elérhessék és a különböző akadályokat, problémákat, hibákat elhárítsák, megoldhassák. VPN felhasználó létrehozásának rendje a következő:

a) Az Intézményi hálózathoz való kapcsolódási szándékot jelezni kell a Gazdasági igazgatónak

b) Az adminisztrátor létrehozza a VPN felhasználót/ jelszót és megosztja az igénylővel

c) a VPN hozzáférés alaphelyzetben le van tiltva

d) a VPN elérés engedélyezése az adott munkanapra szól, az Intézményi munkaidőhöz igazítva

e) Többtényezős hitelesítést kell alkalmazni a különleges jogosultsághoz kötött – úgynevezett privilegizált – felhasználói fiókokhoz való, hálózaton keresztüli hozzáféréshez

f) a VPN elérés csak Intézményi munkaidőben érhető el, az ezen kívüli használatot külön igényelni kell az Intézmény vezetőjétől.

(5) Rendszer- és információsértetlenségre vonatkozó védelmi intézkedések

Rendszer- és információsértetlenségre vonatkozó védelmi intézkedéseket az Intézmény saját üzemeltetésű elektronikus információs rendszerein be kell vezetni. Amennyiben az érintett rendszert külső szervezet üzemelteti, jelen védelmi intézkedésekre vonatkozó követelménye-

ket az. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni és azokat a szolgáltatónak kell biztosítania.

Az elektronikus információs rendszerek hibáit fel kell tárni és tervezetten meg kell javítani. Ennek kapcsán:

a) Az Intézmény valamennyi munkatársának kötelezettsége, hogy az elektronikus információs rendszerek észlelt hibáit bejelentse.

b) A bejelentéseket értékelni, a hibák javítását azok súlyossága alapján priorizálni, majd megtervezni, megrendelni vagy saját hatáskörben elvégezni a hibajavítást.

c) Telepítés előtt a hibajavítással kapcsolatos szoftverfrissítéseket tesztelni kell a feladatellátás hatékonysága, a szóba jöhető következmények szempontjából.

27. § Rendszer frissítések kezelése:

a) az operációs rendszerek, hálózatkezelő eszközök szoftverei, adatbázis-kezelők, egyéb dobozos és egyedi fejlesztésű szoftverek biztonsági frissítéseit a gyártó által történő kiadáskor kockázati értékelésnek kell alávetni. Meg kell állapítani a valós fenyegetettség mértékét és annak függvényében kell dönteni a frissítések bevezetéséről.

b) A kiszolgálók és a munkaállomások operációs rendszereinek frissítései ütemezhetők, kockázatkezelést és tesztelést követően tervezett határidőn belül telepítésre kell, hogy kerüljenek.

c) Egyedi és dobozos feldolgozó szoftverek (számviteli alkalmazások, bér program stb.) frissítéseit a szoftver fejlesztőjével/támogatójával egyeztetett módon kell bevezetni.

d) Nagyobb, több rendszert érintő rendszerfrissítéseket – például adatbázis kezelők frissítései – körültekintően meg kell tervezni, figyelembe véve az összes kapcsolódó rendszerre gyakorolt esetleges hatásait. Amennyiben inkompatibilitási okokból nem valósítható meg a frissítés rövid határidőn belüli telepítése, akkor helyettesítő intézkedéseket (kompenzációs kontrollt) kell bevezetni a végleges megoldásig (például alkalmazás tűzfal telepítése).

A hibajavítást a konfigurációkezelési folyamatba be kell építeni és annak szabályai szerint kell kezelni.

28 § Kártékony kódok elleni védelem

a) Ki kell alakítani a kártékony kódok elleni védelmet olyan módon, hogy az elektronikus információs rendszert annak belépési és kilépési pontjain védje a kártékony kódok ellen, derítse fel és semmisítse meg azokat.

b) A kártékony kódok elleni védelmi mechanizmusokat frissíteni kell minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg. A frissítéseket a konfigurációkezelési szabályaival és eljárásaival összhangban kell elvégezni.

c) A kártékony kódok elleni védelmi mechanizmusokat úgy, kell konfigurálni, hogy a védelem eszköze:

ca.) rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a

végpontokon, a hálózati belépési, vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

cb.) a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt; és riassza a kijelölt rendszeradminisztrátort és a meghatározott további személy(eke)t.

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

29. § Az elektronikus információs rendszer felügyelete

a) Ki kell alakítani az elektronikus információs rendszer felügyeleti rendszerét, amely alkalmas arra, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;

b) Azonosítani kell az elektronikus információs rendszer jogosulatlan használatát;

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

d) A többi naplóinformációhoz hasonlóan, védeni kell a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

e) Meg kell erősíteni az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelek észlelhetők;

f) Biztosítani kell, hogy az elektronikus információs rendszer felügyeleti információkat a kijelölt felelős személyek meghatározott gyakorisággal megkapják.

30. § Biztonsági riasztások és tájékoztatások

a) A kiberbiztonság fenntartása, a biztonsági események és sérülékenységek hatékony kezelése érdekében együtt kell működni a kormányzat elektronikus biztonságért felelős szerveivel:

b) Folyamatosan figyelni kell a kormányzati eseménykezelő központ (GovCert) által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;

c) Folyamatosan figyelemmel kell kísérni a Nemzeti Elektronikus Információbiztonsági Hatóságtól (NEIH) érkező értesítéseket;

d) Szükség esetén belső biztonsági riasztást és figyelmeztetést kell kiadni, melyet el kell juttatni a szervezeten belül az illetékes személyekhez;

e) Ki kell alakítani és működtetni a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, folyamatosan fenn kel tartani a kapcsolatot az érintett, jogszabályban meghatározott szervekkel (GovCert, NEIH);

f) Meg kell hozni a megfelelő ellenintézkedéseket és válaszlépéseket.

31. § A kimeneti információ kezelése és megőrzése

Az Intézmény gondoskodik róla, hogy az elektronikus információs rendszerinek kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel össz-

hangban kerüljenek kezelésre és megőrzésre. A kimeneti információkra vonatkozó megőrzési kötelezettségeket a szakmai és jogi területek állapítják meg, az információk megőrzéséről és kezelésről pedig az informatikus gondoskodik.

32. § Adatvédelmi incidens

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. Amint az adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

33. § Jelentés biztonsági eseményekről

Az információbiztonsági eseményeket a lehető leggyorsabban jelenteni kell az informatikusnak vagy a munkahelyi vezetőnek.

Biztonsági sértésre utalhat, melyet a felhasználóknak azonnal jelenteniük kell, ha

a) szolgáltatás, a berendezés vagy az eszközök elvesztése történik,

b) rendszer rendellenes működését észlelik,

c) a szabályzatoknak vagy irányelveknek való nem-megfelelés válik nyilvánvalóvá,

d) észlelhető a fizikai biztonsági rendelkezések megsértése,

e) nem ellenőrzött rendszerbeli változásokat tapasztalnak,

f) a szoftver vagy hardver hibás működése lép fel,

g) hozzáférési sértések történnek.

A felhasználók tudatossági oktatásában ki kell térni arra, hogy hogyan kell válaszolniuk egy-egy felmerült incidensre, s milyen módon kell elősegíteniük a bizonyítékok gyűjtését.

34. § (1) Jelentés a biztonsági sérülékenységekről

Minden alkalmazott és a külső munkatárs kötelessége, hogy az informatikai rendszerekben általa észlelt rendellenességet, gyaníthatóan gyenge pontot vagy sérülékenységet jelentse az informatikusnak. Ezek a gyenge pontok támadásra, visszaélésre adnak lehetőséget, a védelmi intézkedések meghozatala szükséges. A munkatársak csak jelentsék az észlelt problémát. de ne kíséreljék meg ellenőrizni vagy javítani a feltárt problémát, mert esetlegesen azzal is kárt okozhatnak.

(2) A biztonsági eseményekre és incidensekre adott válasz és fejlesztés

Az észlelt információbiztonsági eseményekre és gyengeségekre mielőbb válaszintézkedéseket kell hozni. Az események követését és a megoldási javaslatok, fejlesztések kidolgozását az informatikus végzi, a jegyzőnek írásban beszámol az ezzel kapcsolatos tevékenységéről.

Amennyiben az esemény komplexebb és speciális szakértelmet igényel, a megoldás kidolgozásához külső szakértőt kell igénybe venni.

(3) Tipikusan információbiztonsági incidensek közé kell sorolni:

a) információrendszer-hibáit és a szolgáltatás megszakadását,

b) rosszindulatú kód, vírustámadás fellépését,

c) DOS támadást (szolgáltatás megtagadása),

d) a nem teljes vagy nem pontos működési adatokból eredő hibákat,

e) a bizalmasság és sértetlenség megsértését,

f) az információrendszerekkel való visszaélést.

(4) Információbiztonsági incidensek esetén az elektronikus információs rendszerek biztonságáért felelős személy irányítja az intézkedéseket:

a) incidens megoldó team összehívása – informatikusok és az érintett területi vezetők bevonása

b) incidens okának felderítése,

c) bizonyítékok gyűjtése,

d) incidens behatárolása és megszüntetése, helyreállítás,

e) előfordulás okának meghatározása és megszüntetése,

f) helyesbítő tevékenység az újbóli előfordulás megakadályozására,

g) tevékenységek dokumentálása,

h) adatközlés az érintettek felé,

i) jelentés a főigazgató felé

(5) Okulás a biztonsági eseményekből

A biztonsági események elemzése alkalmas arra, hogy a fennálló védelmi intézkedéseket hatékonyan felül lehessen vizsgálni és javítani.

A kiértékelés jelezheti az ellenőrzések és eszközök kiegészítésének szükségességét, hogy a jövőben előfordulások valószínűségét csökkenteni lehessen, megelőzve az anyagi és erkölcsi károkozást.

(6) Bizonyítékok gyűjtése

Információbiztonsági események, visszaélések esetén, fegyelmi felelősségre vonás, polgári- vagy büntetőjogi eljárás kezdeményezése csak akkor lehetséges, amennyiben bizonyító erejű dokumentálás történik.

A dokumentálás akkor bizonyító erejű, amennyiben az hiteles és megváltoztathatatlan. Meg kell őrizni a vonatkozó naplóbejegyzéseket, adathordozókat és a papír alapú dokumentumokat is, gondoskodva a bizonyítékok megváltoztathatatlanságáról.

XIII. Fejezet

Ügymenet folytonosság tervezése

35. § (1) Az informatikai szolgáltatások, vagy azok egy részének elvesztése az Intézmény számára katasztrófát jelenthet.

Az informatikai katasztrófa egy olyan nem tervezett esemény, amely az adatfeldolgozó képesség elvesztését okozza hosszabb, legalább 1 munkanap időre. Az ügymenet folytonosság tervezésének az a feladata, hogy a szervezet kritikus információ-feldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal egy informatikai katasztrófa után.

Tekintettel az Intézmény munkafolyamatainak informatikai támogatottságára, az informatikai szolgáltatások elvesztése az érintett munkafolyamatok szinte teljes leállásával jár. Katasztrófa esetén az Intézmény adatvagyona is sérülhet. Elsődleges prioritás az adatvagyon megőrzése, másodlagos az ügyfélfogadás és az azzal kapcsolatos ügymenetek biztosítása. Minden további feladat harmadlagos jellegű.

(2) Tevékenység-sorozat katasztrófa esetén:

a) Az esemény bekövetkezte.

b) A katasztrófa-elhárítási csapat riasztása.

c) A károk enyhítése.

d) A helyreállítási folyamat megindítása.

e) Az alaptevékenység visszaállítása.

f) Tényleges helyreállítás.

g) A tanulságok levonása.

(3) Kritikus informatikai szolgáltatások tekintettel arra, hogy az Intézményben lévő alkalmazások és munkafolyamatok folyamatosan változnak és rendkívül széles körűek, definiálni kell, hogy milyen alkalmazások tekinthetők kritikusnak.

a) Egy adott informatikai szolgáltatás akkor kritikus, ha leállása esetén egyes ügyfelekkel kapcsolatos ügyek nem bonyolíthatók még papír alapú nyilvántartások segítségével sem az előírt Intézményi határidőn vagy az ügyfél által megszokott ügyintézési határidőn belül. Egy ilyen alkalmazás leállása akkor informatikai katasztrófa, ha:

- nem tervezett a leállása;
- tervezett leállása túllépte a maximális 1 nap vagy 1 hétvége időtartamot.

b) Kritikus informatikai szolgáltatás továbbá az, mely az 1. pontba nem tartozik, de nyilvántartása az Intézményi adatvagyon részét képezi, és ez az adatvagyon rész nem érhető el legalább 3 napon keresztül. Ekkor a 3. nap után a szolgáltatás leállása szintén informatikai katasztrófának minősül.

(4) Az informatikai szolgáltatás visszaállításának időtávja

Informatikai katasztrófa bekövetkezése esetén a katasztrófa elhárítását azonnal meg kell kezdeni. Amennyiben az informatikai szolgáltatás nem állítható helyre 2 napon belül, abban az esetben további 3 napon belül meg kell oldani az informatikai vagy papír alapú ideiglenes szolgáltatást. Az ideiglenes szolgáltatás időtávja addig tart, amíg az informatikai szolgáltatás helyreállítása be nem fejeződik, melynél törekedni kell arra, hogy 2 héten belül fejeződjön be.

36. § A szolgáltatás fenntartásának/helyreállításának eszközei

a) Munkaerő

Informatikai katasztrófa bekövetkezése esetén az érintett szervezeti egységek vezetőinek munkaidőn kívül és munkaszüneti napokon is azonnal be kell jönnie az Intézménybe és meg kell kezdenie a szolgáltatás fenntartását/helyreállítását. A helyreállítási munka vezetője a Gazdasági igazgató. Szükség esetén az érintett szervezeti egységek vezetői a vezetésük alatt lévő szervezeti egység személyi állományából további munkatársakat is behívhatnak, akiknek ez esetben szintén kötelező megjelenni. A katasztrófa elhárításáig a munkatársak munkaideje napi 10 óra, munkaszüneti napokon is. Ez alól felmentést vagy engedményt csak a Intézmény vezető adhat.

b) Ideiglenes nyilvántartások

A katasztrófa elhárításának elhúzódó időtartama alatt amennyiben lehetséges és nem veszélyezteti a leállt szolgáltatás adatvagyonának jövőbeli integritását, ideiglenes nyilvántartást kell létrehozni a szolgáltatás helyettesítésére, mely lehet informatikai, de papír alapú is. Az elhárítás befejezése után az ideiglenes nyilvántartás adatainak a helyreállított szolgáltatásba történő integrálását azonnal meg kell kezdeni.

XIV. Fejezet

Naplózás és elszámoltathatóság

37. § Monitorozás

Az elektronikus információs rendszerek figyelemmel kísérésének eszköze az eseménynaplók adatainak gyűjtése és feldolgozása. Be kell vezetni a felhasználói tevékenységekre és a technikai eseményekre vonatkozó naplózást is.

A naplógyűjtést és feldolgozást oly mértékben automatizálni kell, hogy a kritikus események nyomán riasztás keletkezzen és a rendszeradminisztrátorok haladéktalanul tudjanak intézkedni.

38. § Naplózási eljárásrend

Létre kell hozni az Informatikai területen a naplózás részletszabályait tartalmazó naplózási eljárásrendet, amelyben a naplózás és a hozzá tartozó ellenőrzések megvalósulását segíti.

39. § (1) A rendszer használat monitorozása

Az informatikai infrastruktúra működésének és felhasználásának ellenőrzésére felügyeleti eszközöket kell alkalmazni, amelyek probléma esetén meghatározott módon riasztást adnak az illetékes rendszergazda számára. A megfigyelendő paramétereket és riasztási értékeket kockázatértékelés alapján kell meghatározni, meg kell határozni a naplózható és naplózandó eseményeket, s erre fel kell készíteni az elektronikus információs rendszert.

(2) A megfigyelések terjedjenek ki technikai paraméterek ellenőrzésére, továbbá az eszközökhöz és szolgáltatásokhoz történő hozzáférésre is.

Az alábbi események naplózását feltétlenül be kell állítani, amennyiben az alkalmazás ezt lehetővé teszi:

a) a felhasználók tevékenysége,

b) az adatállományok (adatbázisok) módosítása az alkalmazói rendszerekben,

c) lekérdezések és jogosulatlan lekérdezési kísérletek,

d) az üzemeltetők operációs rendszerbe történő be-és kijelentkezése,

e) az üzemeltetők tevékenysége az operációs rendszerben,

f) a hozzáférési jogosultságok módosítása,

g) operációs rendszer események, esetleges hibák,

h) hálózati menedzsment riasztások,

i) konfigurációs beállítások módosítása,

j) jogosulatlan hozzáférési kísérletek, az egyes rendszerek detektálási képességein belül.

A naplózható események fedjék le az alkalmazások működését és az alapinfrastruktúrát oly mélységben, hogy megfelelőek legyenek a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

A naplóbejegyzésekben legyen elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

(3) Napló információk védelme

A naplóinformációk keletkezésük után is szükségesek lehetnek az üzemeltetési vagy információbiztonsági incidensek utólagos kiértékelése céljából, továbbá illegális beavatkozások esetén azok bizonyítására is felhasználhatók.

A naplóinformációkat a naplókezelő eszközöket meg kell védeni a jogosulatlan hozzáféréstől és az utólagos megváltoztatástól vagy törléstől. Meg kell oldani, hogy a rendszeradminisztrátorok ne tudják utólagosan módosítani a naplóbejegyzéseket, és ezzel a saját tevékenységükre vonatkozó információkat megmásítani.

A naplóbejegyzéseket napi gyakorisággal ellenőrizni és elemezni kell a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából. Rendellenes jelenség esetén azt jelenteni kell az illetékes vezetőknek. (informatikai, gazdasági)

Amennyiben jogszabály egyes esetekben másképp nem rendelkezik, a naplóállományokat legalább egy évig meg kell őrizni.

(4) Naplógenerálás és ellenőrzés

A naplózó funkcionalitásnak biztosítania kell naplóbejegyzés generálását az előre meghatározott, naplózható eseményekre. A naplózott eseményeket az arra feljogosított rendszeradminisztrátorok állíthatják be.

A normálistól eltérő működési jellemzők megállapítása az üzemeltető feladata.

Az egyes naplók tartalmának ellenőrzését, kiértékelését előre meghatározott ütemtervnek megfelelően kell végezni, a feljegyzésre kerülő események mennyisége alapján megállapított gyakorisággal. Az ellenőrzéseket az adott rendszerek üzemeltetői végzik. Az ellenőrzések elvégzését dokumentálni kell. Az ellenőrzés végrehajtását az informatikai vezető háromhavonta felülvizsgálja. A felülvizsgálat tényét, és az esetleges megállapításokat jegyzőkönyvben kell rögzíteni.

(5) Naplózási hibák kezelése

Az elektronikus információs rendszerek naplózó funkciójának alkalmasnak kell lennie arra, hogy az informatikai alkalmazás és infrastruktúra naplózási hibája esetén riasztást küldjön az illetékes rendszergazdának, s ezzel párhuzamosan végrehajtsa azokat a tevékenységeket, amelyeket a rendszer biztonságának fenntartása érdekében el kell végezni (például rendszer leállítás, régi naplóbejegyzések felülírása, naplózás leállítása)

(6) Időszinkronizálás

Az Intézmény információ-feldolgozó rendszerének óráit egymással, illetve egy hiteles külső időforrással szinkronizálni kell.

A rendszeres szinkronizálás azért szükséges, mert a berendezések belső órái eltolódnak, továbbá más módon nem biztosítható azok együttes működése.

Ez szükséges lehet üzemeltetési események kivizsgálásánál, vagy bizonyítékként jogi vagy fegyelmi esetekben. A nem szinkronizált bejegyzések akadályozhatják ezeket a kivizsgálásokat és árthatnak az ilyen bizonyíték hitelességének.

A szervezeten belül ki kell jelölni egy pontos idő szervert, vagy szervereket, amelyekhez a többi berendezést szinkronizál. Az idő-szerver a pontos időt lehetőség szerint valamelyik hitelesített külső NTP szerverről kérje le.

XV. Fejezet

XVI. Fejezet

A közérdekű adatok kezelésével kapcsolatos adatvédelmi rendelkezések

42. § A közérdekű adatok kezelése során értelemszerűen alkalmazni kell az AIBSZ szerinti általános adatkezelési szabályokat.

43. § A kötelezően közzéteendő közérdekű adatok közzétételének részletes eljárásrendjét, továbbá a közérdekű adatok megismerésére irányuló kérelmek intézésének rendjét külön szabályzat, nevezetesen az Közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló Szabályzata tartalmazza.

XVII. Fejezet

Záró rendelkezések

44. § Az IBSZ felülvizsgálatát el kell végezni

a) Az IBSZ tárgykörét érintő jogszabály módosítása esetén,

b) Minden olyan esetben, amikor az elektronikus információs rendszerekben, vagy a működési környezetben jelentős változás történik,

c) Évente, tervezetten.

Jelen szabályzat előírásait 2019. január 01-től kell alkalmazni.

Budapest, 2019. január 03.

Kissné Márté Zsuzsanna

intézményvezető