MÁDL FERENC ÖSSZEHASONLÍTÓ JOGI INTÉZET

DR. SZILÁGYI JÁNOS EDE
hivatalvezető

Ikt. szám: IF-MFI/65/5/2020.

A Mádl Ferenc Összehasonlító Jogi Intézet hivatalvezetőjének 4/2020. (VI. 29.) sz. utasítása a Mádl Ferenc Összehasonlító Jogi Intézet informatikai biztonsági szabályzatáról

A MÁDL FERENC ÖSSZEHASONLÍTÓ JOGI INTÉZET INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

I. fejezet

ÁLTALÁNOS RÉSZ

1 Bevezetés

1.1 Az informatikai biztonság az elektronikus információs rendszer olyan állapota, amelynek védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és annak vonatkozó végrehajtási rendeleteinek tartalmával összhangban biztonsági elveket, követelményeket és szabályokat tartalmaz a Mádl Ferenc Összehasonlító Jogi Intézet (a továbbiakban: intézet) adatait kezelő informatikai rendszereket felhasználó személyek számára az informatikai biztonság megteremtése, fenntartása és fejlesztése érdekében.

2 Az IBSZ célja

2.1 Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, valamint megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt, a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig terjedő életciklusukban.

2.2 Az IBSZ-ben szereplő követelményeket, rendelkezéseket a hatályos jogszabályok, elsősorban az Ibtv., valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet [a továbbiakban: 41/2015. (VII. 15.) BM rendelet] keretei között kell alkalmazni az elektronikus információs rendszerek tekintetében megkövetelt biztonsággal, sértetlenséggel és rendelkezésre állással kapcsolatos alábbi célok elérésére:

2.2.1 a jogkövető magatartás és a szervezeti jó hírnév érdekében védeni a szervezet információs vagyonát az adatvédelem és adatbiztonság feltételeinek megteremtése útján;

2.2.2 a tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az informatikai biztonságot, elősegíteni az üzemeltetett

informatikai rendszerek rendeltetésszerű használatát, valamint az adatállományok tartalmi és formai épségének megőrzését;

2.2.3 a megelőzés, a tájékoztatás, az oktatás, a felderítés és az együttműködés eszközeivel segíteni az informatikai rendszerek zavartalan üzemeltetésének folyamatos biztosítását.

3 Az IBSZ tartalma

3.1 Az IBSZ az intézet szervezeti szintű informatikai biztonsági szabályozó rendszerének egyik alapvető eleme. Az IBSZ a hatályos jogszabályokkal, az intézet működési és ügyrendi előírásaival összhangban megteremti az elektronikus információ kezelésének és felhasználásának biztonságát.

3.2 Az IBSZ tartalmazza:

3.2.1 az intézet által használt, a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet alapján a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: kormányzati informatikai szolgáltató) mint üzemeltető és a Belügyminisztérium közötti közszolgáltatási szerződés alapján üzemeltetett elektronikus információs rendszerekkel kapcsolatba kerülő személyek felé támasztott informatikai biztonsági követelmények minimumát a rendelkező részben, továbbá az 1. függelékben meghatározott Felhasználói Informatikai Biztonsági Házirendben;

3.2.2 azokat az elvárásokat, kötelezettségeket és a felelősségi kört, amelyekre az elektronikus információ kezelésének és felhasználásának biztonsága érdekében szükség van;

3.2.3 az elektronikus információk bizalmasságát, hitelességét és rendelkezésre állását biztosító tevékenységek szabályozását és az ezen feltételek biztosítását elősegítő intézeti védelmi intézkedéseket a rendelkező részben, továbbá a biztonsági események és sérülékenységek felhasználói bejelentésére a 2. függelékben, az intézet elektronikus információs rendszereivel kapcsolatos szervezeti hozzáférés szabályozásának eljárásrendjére a 3. függelékben, az elektronikus információbiztonsági kockázatelemzési és kockázatkezelési eljárásrendre a 4. függelékben, valamint a biztonsági események kezelésére irányadó tervre az 5. függelékben meghatározottak szerint.

4 Az IBSZ hatálya

4.1 Az IBSZ területi hatálya kiterjed az intézeti szervezeti egységek elhelyezésére szolgáló épületekre, továbbá olyan épületekre és helyiségekre, amelyekben a 4.2. pontban meghatározott tárgyi hatály alá tartozó elektronikus információs rendszereket, valamint az ezek működését elősegítő eszközöket és programokat használnak, illetve ezekhez kapcsolódó adatkezelést végeznek.

4.2 Az IBSZ tárgyi hatálya kiterjed:

4.2.1 az intézeti feladatellátás körében keletkező elektronikus adatok teljes körére, az intézet adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes elektronikus információs eszközre és ezek működési környezetére, ideértve a kormányzati

informatikai szolgáltató által biztosított és üzemeltett eszközöket, valamint a távoli munkavégzéshez használt eszközöket és ezek működési környezetét is;

4.2.2 a 4.2.1. pontban meghatározottakra vonatkozó bármely dokumentációra;

4.2.3 a 4.2.1. pontban meghatározottak működéséhez alkalmazott szoftverekre, illetve az elektronikus információs eszközökkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

4.3 Az IBSZ tárgyi hatálya nem terjed ki a minősített adatokat kezelő elektronikus információs rendszerekre és a minősített adatokra.

4.4 Az IBSZ személyi hatálya kiterjed az intézetnél munkavégzésre irányuló bármely jogviszonyban álló, az intézet elektronikus információs rendszereivel kapcsolatba kerülő, azokat telepítő, üzemeltető, javító, fejlesztő és használó természetes és jogi személyekre (a továbbiakban külön megnevezés hiányában: felhasználók).

II. fejezet

SZERVEZETBIZTONSÁG

5 Az informatikai biztonsággal kapcsolatos feladatkörök ellátása

5.1 Az intézeti informatikai biztonsággal kapcsolatos feladatkörök ellátásában a szervezeti elektronikus információs rendszerek és eszközök használatával kapcsolatos alábbi szereplők érintettek:

5.1.1 Az intézet vezetőjeként, az informatikai biztonsági szerepkörök és felelősség meghatározása, és ezáltal az intézet elektronikus információs rendszereinek védelméről az Ibtv. 11. § *b), f) és g)* pontjában meghatározottak útján való gondoskodás tekintetében a hivatalvezető;

5.1.2 az Ibtv. 11. § (1) bekezdés *c)* pontja szerinti igazságügyi minisztériumi (a továbbiakban: IM) informatikai biztonsági vezető (a továbbiakban: IBV);

5.1.3 általános vezetői felelősség körében az intézet hivatalvezető-helyettese és szervezeti egységeinek vezetői;

5.1.4 a kormányzati informatikai szolgáltató/központi üzemeltető.

5.2 A hivatalvezető

5.2.1 Az IBSZ biztonsági szabályainak betartatásáról a hivatalvezető az IM IBV közreműködésével gondoskodik, amelynek keretében:

5.2.2 hatáskörébe tartozóan dönt az informatikai biztonság növelésére tett főbb kezdeményezések elbírálása, valamint az intézet szervezetét érintő informatikai biztonsági intézkedések bevezetése tárgyában;

5.2.3 az IM IBV közreműködésével ellenőrzi az Ibtv.-ben meghatározott informatikai biztonsági követelmények és tevékenységek megfelelőségét.

5.3 Az IM IBV

5.3.1 Az IBV az IM elektronikus információbiztonsági (a továbbiakban: EIB) feladatkör ellátására kijelölt munkatársaival, az EIB feladatkörön belül megszervezi és ellátja a kormányzati informatikai szolgáltatóval, valamint az intézeti szervezet érintett vezetőivel és munkatársaival való kapcsolattartás és koordináció keretén belül az alábbiakat:

5.3.1.1 általános feladatkörében közreműködik az intézet adatait feldolgozó elektronikus információs rendszerek biztonságával összefüggő tevékenységek tervezését, szervezését, koordinációját és ellenőrzését érintő feladatokban;

5.3.1.2 a hivatalvezető ilyen irányú jelzésére és közreműködésével elvégzi az IBSZ legalább évenkénti felülvizsgálatát és szükség szerinti módosításának előkészítését;

5.3.1.3 kapcsolatot tart a Nemzeti Kibervédelmi Intézettel, illetve annak részére a vonatkozó jogszabályi háttérben foglalt kötelező adatszolgáltatásokat az érintettek bevonásával előkészíti és teljesíti;

5.3.1.4 kidolgozza az információbiztonsági tudatosság fejlesztését célzó éves kötelező képzésekre vonatkozó IM szervezeti tervet és az IM Személyügyi Főosztály, valamint a hivatalvezető közreműködésével szervezi és végrehajtja azt az MFI szervezete tekintetében.

5.4 A központi üzemeltető/a kormányzati informatikai szolgáltató

5.4.1 Az intézet részére informatikai szolgáltatásokat nyújtó szervezet elektronikus információs rendszereit üzemeltető munkatársai felelősek az informatikai biztonság fenntartásáért a felügyeletükre bízott elektronikus információs rendszerekben.

5.4.2 Az intézeti elektronikus információs rendszerek működtetéséhez szükséges informatikai alapinfrastruktúra feltételeit biztosító kormányzati informatikai szolgáltató az Ibtv. és annak végrehajtási rendeletei figyelembevételével, a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet 5. § (1) bekezdése szerinti munkacsoport működése során, az IM IBV ilyen irányú tevékenysége útján hangolja össze a kormányzati informatikai üzemeltetés és az intézeti informatikai követelmények megvalósítását.

6 Az intézet által használt használt elektronikus információs rendszerek hozzáférés szabályozásának alapelvei

6.1 Az elektronikus információs rendszer minden meghatározó elemét olyan védelmi mechanizmusnak (fizikai, logikai, adminisztratív) kell védenie, amely megakadályozza az illetéktelen személyek hozzáférését a védett elektronikus információs rendszerhez.

6.2 Az intézet által igénybe vett elektronikus információs rendszerek esetében az üzemeltetői, illetve az adatgazdai feladat és hatáskörrel rendelkező szervezet eljárásrendét kell figyelembe venni az elektronikus információs rendszerre vonatkozó jogosultságigénylés és -kiadás folyamata kapcsán.

6.3 Az intézet saját tulajdonú, üzemeltetésű, illetve adatgazdaként használt elektronikus információs rendszerek esetében a rendszer dokumentációjában rögzített és az MFI által lefektetett eljárásrendek alkalmazandóak.

6.4 Az intézet elektronikus információs rendszereivel kapcsolatos szervezeti hozzáférés szabályozásának eljárásrendjét a 3. függelék tartalmazza.

7 Harmadik fél hozzáférésének alapkövetelményei

7.1 Harmadik félnek minősül az IM és a kormányzati informatikai szolgáltatón kívüli olyan külső szereplő aki külön szerződés alapján az intézet számára informatikai jellegű szolgáltatást nyújt.

7.1.1 Harmadik fél csak egyedi esetben, meghatározott időre és meghatározott feladat megoldásához látható el az intézeti elektronikus információs rendszerekhez kapcsolódó jogosultsággal, amelyet szerződésben kell dokumentálni. A szerződéstervezet EIB szempontú véleményeztetését a hivatalvezetőnek kell kezdeményeznie az IM IBV felé.

7.1.2 Amennyiben a 7.1 szerinti rendelkezés beszerzési típusú szerződésekhez kapcsolódik, akkor a szerződéstervezet EIB szempontú véleményezését az IM Jogi Szolgáltatási Főosztálya kezdeményezi az IM IBV felé, tekintettel az intézet működésével összefüggő egyes feladatok ellátásáról szóló hatályos megállapodásban foglaltak ilyen irányú tartalmára.

7.2 Az intézet és szerződéses partnerei megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

7.3 A harmadik félnek az intézet információs vagyonához történő hozzáférése esetében – figyelembe véve a szükséges hozzáférési típusokat, az információ értékét, a harmadik fél által alkalmazott biztosítékokat, valamint a hozzáférés mélységét – törekedni kell a kockázatok minimalizálására.

7.4 Azokban az esetekben, amelyekben az információ feldolgozása vagy kezelése kiszervezéssel történik, a harmadik féllel kötött szerződésnek a betartandó biztonsági követelményeket is tartalmaznia kell.

7.5 Harmadik fél hozzáférése az intézet adataihoz és információihoz, a munkájához elengedhetetlenül szükséges minimum szintre kell korlátozni. A hozzáférések feltételeit szerződésben kell részletezni. A szerződés csak az Ibtv.-vel, az intézet IBSZ-évél összhangban lévő követelményeket tartalmazhat.

7.6 A szerződésnek tartalmaznia kell továbbá a bizalmasságra, a szellemi tulajdonjogokra, a szerzői jogok átruházására és minden közösen végzett munkálat védelmére vonatkozó garanciákat is.

7.7 A szerződésben elő kell írni, hogy az intézet információs vagyonelemei a szerződés lejártát követően kerüljenek vissza az intézet birtokába, a szerződött félnél – valamint annak partnereinél, alvállalkozóinál – pedig kerüljenek véglegesen törlésre.

7.8 Harmadik fél az anyagokat és információkat a hozzáférést rögzítő szerződés vagy titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

7.9 A szerződéses partnereknek vállalniuk kell, hogy rendszereik a vállalt feladat ellátására alkalmasak. A szerződésben szerepeltetniük kell vészhelyzeti eljárásra vonatkozó pontokat is. Ebben rögzíteni kell a rendelkezésre állás idejét, a reagálási időt, annak

módját és az értesítendők adatait. Rögzíteni kell továbbá a megoldás folyamatát, az elhárítás várható időtartamát, és hatékony jelentési rendszert kell megkövetelni.

7.10 A harmadik féllel kötött szerződés biztonsági követelményei

7.10.1 Az intézetnek az általa használt elektronikus információs rendszereket érintő polgári jogi szerződései az IBSZ hatálya alá tartoznak, ezért azok tartamát az IBSZ rendelkezéseivel összhangban kell meghatározni. A polgári jogi szerződések előkészítése során az alábbiakat kell alkalmazni, illetve figyelembe venni:

7.10.1.1 az Ibtv. és a 41/2015. (VII. 15.) BM rendelet rendelkezéseit;

7.10.1.2 az intézeti IBSZ rendelkezéseit;

7.10.1.3 az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának biztonsági osztályba sorolását;

7.10.1.4 a sérülékenység-vizsgálatra vonatkozó kikötést;

7.10.1.5 az információk másolásának és nyilvánosságra hozatalának feltételeit;

7.10.1.6 a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;

7.10.1.7 a felek felelősségének meghatározását;

7.10.1.8 a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;

7.10.1.9 a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

7.10.1.10 a felmerülő problémák kezelését;

7.10.1.11 a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;

7.10.1.12 világos és egyértelmű jelentéskészítési struktúrát és rendszert;

7.10.1.13 a változáskezelések egyértelmű és meghatározott folyamatát;

7.10.1.14 óvintézkedések meghatározását a kártékony kódok ellen, és a védelmi intézkedések meghatározását a biztonsági események kezelésére;

7.10.1.15 biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását.

III. fejezet

SZEMÉLYI BIZTONSÁG

8 A munkaköri felelősség és az alkalmazás feltételei

8.1 A 4.4. pontban foglalt felhasználókat az intézettel kapcsolatos jogviszonyuk szerint az IBSZ tartalmával meg kell ismertetni, a megismerésről szóló írásbeli nyilatkozat tételével, legkésőbb a jogviszonyt létesítő okirat átadásával egyidejűleg.

8.2 Az intézettel munkavégzésre irányuló jogviszonyban álló felhasználók munkaköri leírásaiban meg kell határozni az általános és az adott munkakörhöz tartozó informatikai biztonsági feladatokat és felelősségeket.

8.3 A felhasználók kötelezettségeit, felelősségeit az 1. függelékben meghatározott Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) tartalmazza.

8.4 Az intézetnek a munkakörbe való belépéskor az intézeti Közszolgálati Szabályzat és az IBSZ elérhetőségének biztosításával, valamint az évente rendszeresen megtartott IM elektronikus információbiztonsági képzések útján tájékoztatnia kell a munkatársakat arról, hogy milyen jogi felelősségük és kötelezettségük van az informatikai biztonsági előírások betartására vonatkozóan, továbbá a munkáltatónak az általa biztosított munkaeszközökre és informatikai infrastruktúrára vonatkozó ellenőrzési jogosultságairól. Az intézeti munkatársak informatikai biztonsági felelőssége arra az esetre is vonatkozik, ha nem az intézetben (pl. távoli hozzáférés, otthoni munka, távmunka), illetve munkaidőn kívüli, EIB érintettséggel rendelkező munkavégzés történik.

8.5 A titoktartási nyilatkozat

8.5.1 Az intézeti elektronikus információs rendszerekkel kapcsolatos tevékenység tekintetében, a külön megállapodásban rögzített ilyen irányú jogviszony által meghatározott kereteken belül az igazságügyi miniszter feladat- és hatáskörét érintően a nemzetbiztonsági ellenőrzés alá eső személyek meghatározásáról szóló 7/2015. (IV. 10.) IM rendelet 3. §-ában, 4. §-ában és 1. mellékletében meghatározott, az intézet informatikai hálózatán, illetve elektronikus információs eszközein és rendszerein munkát végző érintett munkatársakon túl, az ilyen tevékenységre jogosult harmadik fél eljáró képviselői is titoktartási nyilatkozat tételére kötelezettek.

8.6 Az informatikai biztonság szervezeti oktatása és képzése

8.6.1 Az IM IBV az IM oktatási és képzési terve szerint évenkénti rendszeres belső oktatásokkal gondoskodik arról, hogy a felhasználókban tudatosodjanak az alapvető informatikai biztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő informatikai biztonsági fenyegetettségeket, és ezzel felkészültek legyenek a FIBH-ban foglaltak betartására.

8.6.2 Az oktatási és képzési tervben kiemelt jogosultságokkal megjelölt munkatársak részére külön oktatást kell biztosítani az intézeti elektronikus információs rendszerekkel kapcsolatos szerepük függvényében.

8.6.3 Az oktatáson, illetve továbbképzésen való részvétel az elektronikus információs rendszer minden szintű felhasználója számára kötelező, a megjelenést a résztvevők aláírásukkal igazolják az IM Személyügyi Főosztály felé a jelenléti íven.

IV. fejezet

FIZIKAI BIZTONSÁG

9 Az irodák, a helyiségek és az eszközök biztonsága

9.1 A 4.1. pontban foglalt védett intézeti helyiségek védelmét az alábbiak szerint kell elősegíteni:

9.1.1 a kulcsokat nem szabad nyilvános, idegenek számára is könnyen hozzáférhető helyen tárolni;

9.1.2 azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani.

9.2 Harmadik fél munkavégzése biztonságos környezetben

9.2.1 Az intézeti területen dolgozó, ideiglenes jellegű munkát végző harmadik félre vonatkozóan, a 7.10. pontban foglaltaknak megfelelően elő kell írni, hogy számukra a hozzáféréseket csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani.

9.3 Az elektronikus információs eszközök biztonsága és karbantartása

9.3.1 Az információs vagyon – lopás, veszélyeztetés, egyéb károsodás elleni – védelmének és a működési folyamatok folytonosságának biztosítása érdekében az intézet elektronikus információs eszközeit, azok megfelelő, illetéktelenek hozzáférését kizáró megoldású fizikai elhelyezésével és kezelésével is biztosítani kell.

9.3.2 Az elektronikus információs eszközök elhelyezése és védelme

9.3.2.1 Az elektronikus információs eszközöket úgy kell elhelyezni, és védelmüket úgy kell kialakítani, hogy minimálisra csökkenjenek a környezeti hatások következtében megjelenő kockázatok, és minimálisra csökkenjen az illetéktelen hozzáférések lehetősége, de a munkavégzés hatékonysága ne romoljon.

9.3.2.2 A védelmi intézkedéseknek biztosítaniuk kell, hogy a különböző környezeti hatások miatt keletkező meghibásodások rendszerekre gyakorolt hatásának súlyossága csökkenjen. Ezért

9.3.2.2.1 be kell tartani a tűzvédelmi előírásokat;

9.3.2.2.2 a monitorokat úgy kell elhelyezni, hogy ki lehessen zárni azok illetéktelen személy általi leolvasását.

9.3.3 Az elektronikus információs eszközök intézeten kívüli biztonsága

9.3.3.1 Az intézet területén kívüli elektronikus információs eszközök használatát a legszükségesebb mértékűre kell korlátozni. Hivatali munkavégzésre elsődlegesen az intézet vagy a kormányzati informatikai szolgáltató tulajdonát képező hordozható elektronikus információs eszköz használata engedélyezhető. A hordozható elektronikus információs eszköz felhasználókra vonatkozó részletesebb biztonsági előírásait a FIBH tartalmazza.

9.3.4 „Üres asztal – üres képernyő" szabály

9.3.4.1 Az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden munkatársnak ismernie és alkalmaznia kell a FIBH 9.2. „Üres asztal – üres képernyő" pontjában leírtakat.

9.3.5 Az infokommunikációs eszközök karbantartása

9.3.5.1 A folyamatos működés érdekében az intézet elektronikus információs eszközeinek karbantartása és ellenőrzése a kormányzati informatikai szolgáltató saját, az IBSZ rendelkezéseivel összhangban lévő eljárása szerint történik.

9.3.6 Az elektronikus információs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása előtt a szolgáltatónak vagy az eszközt biztosító szervezetnek saját eljárása szerint minden esetben gondoskodnia kell arról, hogy az elektronikus információs eszközökön tárolt információk visszaállíthatatlanul eltávolításra kerüljenek.

V. fejezet

AZ INTÉZET BIZTONSÁGI SZINTBE SOROLÁSA

10 Az intézet biztonsági szintbe sorolása

10.1 Az intézet biztonsági szintje a 41/2015. (VII. 15.) BM rendelet 2. melléklet 4. pontjában foglalt előírások alapján 2-es szintnek megfelelően került megállapításra.

VI. fejezet

ZÁRÓ RENDELKEZÉSEK

11 Hatálybalépés és közzététel

11.1 Az IBSZ az aláírását követő napon lép hatályba.

11.2 Az IBSZ-t az MFI internetes honlapján (http://mfi.gov.hu/hu/) közzéteszi.

Budapest, 2020. június 29.

Wáldl Ferenc Összehasonlító Jogi Intézet
* 1 *

Dr. habil. Szilágyi János Ede PhD.
hivatalvezető

1. függelék a 4/2020. (VI. 29.) sz. hivatalvezetői utasításhoz

FELHASZNÁLÓI INFORMATIKAI BIZTONSÁGI HÁZIREND

1 A Felhasználói Informatikai Biztonsági Házirend célja

1.1 A Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) célja, hogy a Mádl Ferenc Összehasonlító Jogi Intézet (a továbbiakban: intézet) elektronikus információs rendszereinek és az intézet részére informatikai szolgáltatásokat nyújtó szervezetek elektronikus információs rendszereinek felhasználói megismerjék a velük szemben támasztott elvárásokat és a biztonsági előírások rájuk vonatkozó részét.

2 A FIBH hatálya

2.1 A FIBH területi, tárgyi és személyi hatálya az IBSZ 4. pontjában foglaltakra terjed ki.

3 Informatikai biztonsággal kapcsolatos szerepkörök

3.1 Az informatikai biztonság folyamatos, a vonatkozó jogszabályokban előírt és az intézet vezetése által elvárt szinten tartása érdekében, az informatikai biztonsággal kapcsolatos intézeti, illetve a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: kormányzati informatikai szolgáltató) felőli szerepkörök az alábbiak szerint kerülnek meghatározásra:

3.1.1 Felhasználó: az IBSZ 4.4. pontjában meghatározott személyi kör.

3.1.2 Üzemeltető: az IBSZ 5.4. pontjában meghatározott személyi kör.

3.1.3 Ügyfélszolgálat, hibaelhárítás.

3.1.3.1 A felhasználók általános informatikai támogatását és a biztonsági eseménynek nem minősülő informatikai hibák kezelését a kormányzati informatikai szolgáltató Ügyfélszolgálata, az intézeti szakrendszerek vonatkozásában pedig az adott szakrendszer szervezeti üzemeltetéséért felelős szervezeti egysége végzi, szükség esetén a kormányzati informatikai szolgáltatóval együttműködésben.

3.1.4 Informatikai biztonsági vezető.

3.1.5 A hivatalvezető az IBSZ 5.2. pontjában foglaltak szerint látja el az intézet informatikai biztonságával kapcsolatos feladatok koordinálását, és felügyeli az intézet informatikai biztonsági szabályozóinak betartását.

4 Az FIBH-ben foglaltak betartása

4.1 A felhasználó az informatikai biztonsági előírások betartásával, az üzemeltető az informatikai biztonsági előírások betartásával és betartatásával megvédi az intézet rendszereinek felhasználóit, partnerei adatait, információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől, illetve csökkenti az esetlegesen bekövetkező kármértéket.

4.2 Az intézet elektronikus információs rendszerei minden használójának folyamatosan be kell tartania jelen FIBH-ban előírtakat és azokat a biztonsági előírásokat, amelyek a kapcsolódó szabályzatokban, utasításokban és eljárási leírásokban jelennek meg, különös tekintettel a kormányzati informatikai szolgáltató ilyen irányú előírásaira. A szabályok be nem tartása jogi, illetve munkaügyi következményeket vonhat maga után. A FIBH ismeretének hiánya nem mentesít a felelősség alól.

4.3 Az intézeti szervezeti egység vezetője közvetlenül felelős azért, hogy az irányítása alá tartozó munkatársak betartsák az informatikai biztonsági előírásokat. Amennyiben alapos gyanú merül fel arra, hogy a felhasználó az intézet elektronikus információs rendszerének felhasználásával foglalkoztatásra irányuló jogviszonyából eredő kötelezettségét megszegte, a munkáltatói jogkör gyakorlója jogosult az ezzel kapcsolatos ellenőrzést elrendelni, és az IM IBV útján és közreműködésével lefolytatni.

4.4 Az ellenőrzés célja az intézeti elektronikus információbiztonsági követelmények megvalósítása céljából a FIBH-ban foglaltak betartásának vizsgálata. Az ellenőrzés során az IM IBV a kormányzati informatikai szolgáltató közreműködését veszi igénybe, amelynek keretében az ellenőrzés tárgyát képezi különösen a felhasználó részére használatba adott informatikai eszköz és a felhasználó tevékenységével összefüggő naplófájlok vizsgálata, valamint a felhasználó hivatali elektronikus levelezésének áttekintése.

5 A felhasználóra vonatkozó szabályok

5.1 A felhasználó kötelezettségei

5.1.1 A felhasználó az intézet elektronikus információs rendszereit csak és kizárólag munkavégzés céljára használhatja. Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítania kell.

5.1.2 Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésére nem jogosult, a hibát a szolgálati út betartásával jeleznie kell az informatikai biztonsági vezetőnek.

5.1.3 Valamennyi felhasználó köteles azonnal értesíteni közvetlen felettesét minden olyan körülményről, amely információbiztonsági incidens bekövetkezésének gyanújára utal. A vezető ilyen esetben a szolgálati út betartásával értesíti az informatikai biztonsági vezetőt, az intézeti vagy szervezeti üzemeltetési egységet, illetve a kormányzati informatikai szolgáltató Ügyfélszolgálatát.

5.1.4 Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosító, jelszó, eToken, kulcs, biometrikus azonosító vagy bárminemű egyéb, az intézet erőforrásaihoz hozzáférést biztosító eszközt.

5.1.5 A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló munkatársak sem közölhetik ezeket egymással, ezek az üzemeltetőnek sem adhatók ki. Azok kompromittálódásának gyanúja esetén azonnali megváltoztatásuk szükséges.

5.1.6 Az informatikai biztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban az érintett felhasználó köteles együttműködni a vizsgálatot lefolytató IM IBV-vel, illetve kijelölt munkatársaival. Amennyiben a kormányzati informatikai szolgáltató kezdeményez vizsgálatot, úgy a felhasználó azt a hivatalvezető útján az IM IBV felé haladéktalanul jelezni köteles.

5.1.7 Az intézet elektronikus információs eszközeinek személyes haszonszerzésre irányuló felhasználása, valamint a szakmai elvárások és magatartás szabályaival ellenkező módon történő felhasználása szigorúan tilos.

5.1.8 A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, más felhasználói jelszavak kipróbálása, illetve ezek kísérlete is.

5.1.9 Az intézeti munkavégzési tevékenység során az alkalmazottak csak az intézet tulajdonát képező, illetve az intézet részére informatikai szolgáltatásokat nyújtó szervezet által biztosított informatikai eszközöket és engedélyezett szoftvereket használhatják munkavégzésre. Ettől eltérni csak a hivatalvezető engedélyével és az IM informatikai biztonsági vezető előzetes jóváhagyásával lehet.

5.1.10 A 3.1.2. pontban hivatkozott informatikai üzemeltetés munkatársait kivéve, a felhasználó semmilyen elektronikus információs eszközt vagy szoftvert nem telepíthet az intézet elektronikus információs rendszerébe, azok elhelyezését, telepítési módját nem változtathatja meg, továbbá semmilyen szoftvert nem futtathat és nem törölhet.

5.1.11 A nyomtatásra, lapolvasásra, fénymásolásra, faxolásra alkalmas készülékek, multifunkcionális eszközök használatánál ügyelni kell arra, hogy

5.1.11.1 az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben;

5.1.11.2 illetéktelenek ne férhessenek hozzá;

5.1.11.3 véletlen vagy szándékos átprogramozás során az üzenetek nehogy egy nem megfelelő számra kerüljenek;

5.1.11.4 félretárcsázás vagy hibásan tárolt szám miatt az üzenetek nehogy illetéktelen személyhez kerüljenek.

5.1.12 A felhasználó felelősséggel tartozik:

5.1.12.1 a szabályok betartásáért;

5.1.12.2 a birtokában lévő vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;

5.1.12.3 az elektronikus információs rendszerben az általa vagy a digitális identitása nevében végzett műveletekért;

5.1.12.4 az intézet elektronikus információs eszközeinek (számítógép, nyomtató, scanner stb.) szakszerű, szabályszerű kezeléséért;

5.1.12.5 a személyi használatra átvett eszközök megfelelő fizikai védelméért.

5.2 A felhasználó jogosultságai

5.2.1 A felhasználó jogosult

5.2.1.1 a számára biztosított elektronikus információs eszközök, szoftverek üzemszerű használatára munkája elvégzése céljából;

5.2.1.2 a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére;

5.2.1.3 rendszeres szervezeti informatikai biztonságtudatossági képzésre;

5.2.1.4 a munkavégzéséhez biztosított informatikai eszközök működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges, általa nem ismert szoftver eszközökhöz támogatás igénylésére;

5.2.1.5 meghibásodás, üzemzavar esetén annak elhárításának az igénylésére.

6 Az információ kezelésének szabályai

6.1 Munkaállomások hozzáférés védelme

6.1.1 A felhasználó a hivatali munkavégzésre használt munkaállomást csak saját nevével és jelszavával belépve használhat.

6.1.1.1 A kormányzati informatikai szolgáltató által biztosított és üzemeltetett munkaállomást harmadik fél csak a munkaállomás nevesített felhasználója szervezeti egysége vezetőjének előzetes írásbeli engedélyével használhatja, ebben az esetben is a saját azonosító használatával. Hibaelhárítás vagy támogatás esetén a kormányzati informatikai szolgáltató támogató munkatársa adminisztrátori azonosítójával és jogosultságával a felhasználó jelenlétében a felhasználó munkaállomására beléphet.

6.2 A hozzáférés-kiosztás folyamata

6.2.1 A kormányzati informatikai szolgáltató által üzemeltetett informatikai rendszerbe belépést lehetővé tevő azonosítót az önálló szervezeti egység vezetője (főosztályvezető) igényli a felhasználóknak, a Szolgáltató erre a célra rendszeresített nyomtatványán.

6.2.2 Az önálló szervezeti egység vezetője (főosztályvezető) által aláírt nyomtatvány Ügyfélszolgálatnak történő átadását követően a tartományi (NISZ tartományába történő) belépést lehetővé tevő azonosítót és a kezdeti jelszót a kormányzati informatikai szolgáltató kirendelt munkatársa személyesen adja át az új felhasználónak, és az átadás során a kezdeti jelszó megváltoztatásáról és az egyéb testreszabási lépésekről oktatásban részesíti a felhasználót.

6.2.3 A kormányzati informatikai szolgáltató átadja a nyomtatványon a vezető által igényelt levelezéssel és a napi munkával kapcsolatos egyéb speciális alkalmazásokkal kapcsolatos belépési és a programok elindításával kapcsolatos alapinformációkat.

6.3 Hozzáférés hálózati erőforrásokhoz és az egyes alkalmazói programokhoz

6.3.1 Az információs rendszerek üzemeltetői felügyelik és ellenőrzik az elektronikus információs rendszerek használatát a rendszerek biztonságos üzemeltetési környezetének fenntarthatósága érdekében.

6.3.2 Az intézet elektronikus információs eszközein működtetett szoftvereket és alkalmazói rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja. A felhasználó a számítógépe és a hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap. Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni.

6.3.3 A felhasználói jelszavak képzésének szabályai

6.3.3.1 a jelszó képzésének meg kell felelnie az üzemeltető szervezet által meghatározott minimum követelményeknek. Javasolt, hogy legalább tíz karakter hosszú legyen, és – ahol az műszakilag megvalósítható – törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

6.3.3.2 a jelszó könnyen megjegyezhető és nehezen kitalálható legyen;

6.3.3.3 a jelszó nem utalhat a felhasználói névre, e-mail-címre, telefonszámra vagy a gépnévre, továbbá olyan személynévre, személyes adatra, amely a megfejtését megkönnyíti;

6.3.3.4 a jelszó nem lehet egyforma betűből vagy számból álló sorozat, és nem tartalmazhatja egymást követő karakterek sorozatát (pl. 111111; aaaaaa; 123456; abcdefg).

6.3.4 A felhasználói jelszavak alkalmazása

6.3.4.1 a felhasználó a jelszavát köteles titokban tartani;

6.3.4.2 a felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben;

6.3.4.3 a felhasználói jelszót tilos leírni és a felhasználói munkaállomás környezetében elhelyezni;

6.3.4.4 ha a jelszó kompromittálódásának gyanúja merülne fel, akkor azt azonnal meg kell változtatni, és értesíteni kell az informatikai biztonsági vezetőt;

6.3.4.5 nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé (pl. makróra vagy funkció billentyűre);

6.3.4.6 a jelszavakat a kormányzati informatikai szolgáltató vonatkozó és automatizált csoportházirendi intézkedése alapján meghatározott időközönként meg kell változtatni, az egyéb információs rendszerekben az üzemeltető előírásainak megfelelően kell eljárni;

6.3.4.7 korábbi jelszavak újra használatát kerülni kell.

6.4 Hozzáférés-védelem mobil elektronikus információs eszköz esetén

6.4.1 A mobilitás miatt sokkal nagyobb veszélynek kitett mobil elektronikus információs eszközök esetében is egyedi azonosítási megoldást (pl. PIN-kód, feloldóminta, biometrikus azonosító, jelszó) kell használni a rendszerbe történő belépéshez.

6.4.2 Szervezeti információk mobil elektronikus információs eszközön hozzáférési védelem nélkül nem kezelhetőek, tárolhatóak.

6.4.3 A munkavégzéssel kapcsolatos feladat elvégzése után a keletkezett adatokat a hálózati meghajtóra kell menteni.

6.4.4 A mobil elektronikus információs eszközökről a feleslegessé vált adatokat haladéktalanul le kell törölni.

6.4.5 Nyilvános helyeken – nem a kormányzati informatikai szolgáltató által biztosított – való hálózat használatnál történő munkavégzés során kerülni kell a nem megbízható, jelszóval nem védett vezeték nélküli hálózatok (free wifi) használatát.

6.4.6 Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

6.5 Adatmentések, az adathordozók nyilvántartása és tárolása

6.5.1 Az adatokat nem az elektronikus információs eszköz saját tárhelyén, hanem a kiszolgálók vagy hálózati tárterületek (kormányzati felhő- vagy hálózati adattároló) megfelelő könyvtáraiban kell tárolni, ahol biztosítható azok rendszeres mentése és biztonságos tárolása.

6.5.2 A megfelelő könyvtárba mentés a felhasználó felelőssége. A helyi gépen tárolt adatokért az üzemeltetők nem vállalnak felelősséget.

6.5.3 A hálózati adattárolón tárolható minden, a munkához szükséges, ahhoz kapcsolódó dokumentum. Minden felhasználó számára rendelkezésre áll a saját belépési azonosítójához rendelt „Dokumentumok" könyvtár a saját adatok tárolására és a „szervezeti egység számára létrehozott könyvtár a közös anyagok tárolására.

6.5.4 A kormányzati informatikai szolgáltató vállalja a felelősséget az általa biztosított hálózati tárhelyeken tárolt adatok rendelkezésre állására, mentésére és biztonságos tárolására.

6.5.5 Szigorúan tilos bármely munkához köthető adatnak vagy munkaanyagnak a nem kormányzati online tárhelyek vagy közösségi média (pl. Facebook, LinkedIn, Dropbox, ToldACuccot, Mammutmail, Mammutshare stb.) igénybevételével való mozgatása vagy tárolása. Ezen célra kizárólag a kormányzati informatikai szolgáltató által biztosított levelező rendszer, illetve egyéb online tárhely használható.

6.5.6 Az üzemeltetők a kiszolgáló megadott könyvtárában tárolt ügyviteli adatokról belső eljárásrendjükben előírt módon és gyakorisággal mentést készítenek. Speciális mentési igényekről az illetékes üzemeltetőt írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

6.5.7 Az adat-visszaállítást az adatgazda írásbeli (e-mail) igénye alapján a feladat végrehajtásában illetékes üzemeltető végzi el.

6.5.8 A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat utoljára ismert pontos helyét, megnevezését.

6.5.9 A szervezeti információkat tartalmazó eszközöket védett területeken kívül olyan módon kell tárolni és szállítani, hogy egy esetleges illetéktelen hozzáférési kísérlet észlelhető és kivédhető legyen.

6.6 Az intézet munkatársainak a közösségi médiában való részvételének általános keretei:

6.6.1 A nem kormányzati online szolgáltatások (webáruház, társkereső szolgáltatás, pénzügyi szolgáltatások stb.) igénybevételéhez a hivatalitól eltérő azonosítók (pl. felhasználónév, e-mail-cím, jelszó) használata kötelező, figyelemmel a kapcsolódó informatikai biztonsági kockázatok fennállására.

6.6.2 Az intézeti munkatársaknak az online térben, a közösségi média különböző területein a hivatali munkaidőn túl is figyelemmel kell lenniük arra, hogy közszolgálati hivatásukkal összefüggésben személyük és adataik ne kompromittálódjanak, támadási felület adta szervezeti biztonsági kockázat kialakulására ne legyen lehetőség.

6.6.3 Tilos a munkaeszközként kiadott mobil elektronikus információs eszközt vagy hozzáférést nem kormányzati online szolgáltatások és közösségi médiatartalmak kezelésére használni, a 6.6.1. pontban foglaltak okán.

6.6.4 Tilos az egyéb munkához köthető események részleteinek (találkozó és rendezvény időpontok és helyszínek), a nem kormányzati online szolgáltatáson keresztüli küldése, tárolása vagy publikálása, ha az biztonsági kockázatot hordoz magában. A munkavégzéshez vagy az intézethez köthető eseményeknek a publikálása – az intézeti szervezeti és működési szabályzatban foglaltak szerint – a sajtóügyekben eljárásra felhatalmazottak kizárólagos feladata.

6.6.5 A 6.6.1.–6.6.4. pontokban foglaltak figyelmen kívül hagyásából eredő személyes, szervezeti vagy egyéb károkért, hátrányokért az adott felhasználó felelőssége áll fent.

6.6.6 A kormányzat informatikai ellátásért felelős szolgáltató szabályozott kereteken belül a 6.6.1.–6.6.3. pontokban foglalt szolgáltatások biztonságos és engedélyezett kiváltására lehetőséget nyújt az általa biztosított kormányzaton belüli, azok szereplői között használható rendszereken keresztül

6.6.6.1 a kommunikációra, azonnali üzenetváltásra (chat funkciót támogató platformon);

6.6.6.2 az események szervezésére, menedzselésére (irodai szoftver használatával);

6.6.6.3 a feladatok kezelésére és ütemezésére (irodai szoftver használatával);

7 Felhasználók számítógépes környezete

7.1 A felhasználói informatikai környezet kezelési előírásai

7.1.1 A felhasználó felelős az elektronikus információs eszközön általa végzett szakszerűtlen beavatkozásának következményeiért.

7.1.2 A felhasználónak elektronikus információs eszköz, illetve szoftver telepítési igényével a kormányzati informatikai szolgáltató Ügyfélszolgálatát kell megkeresnie. Az igénylést a hivatalvezető küldi meg az Ügyfélszolgálat számára az IM IBV jóváhagyását követően.

7.1.3 Az üzemeltető bizonyos szoftverelemek telepítését központi szétosztással, automatikusan végzi, előzetes tájékoztatást követően. Indokolt esetben a felhasználó szervezeti egységének vezetője az IM IBV jóváhagyásával kérheti a frissítés telepítésének egy későbbi időpontban történő elvégzését. A kormányzati informatikai szolgáltató által távolról történő frissítéskor meg kell várni a frissítés befejeződését, a folyamatot leállítani tilos. El kell fogadni, hogy ez alatt az idő alatt a számítógép valamivel lassabban működik, illetve előfordulhat, hogy a számítógép leállása vagy elindulása a javítás telepítését követő első alkalommal hosszabb ideig tart a korábban megszokottnál.

7.1.4 Az intézet belső hálózatához idegen számítógép nem csatlakoztatható.

7.2 Az internet és az elektronikus levelezés használatának főbb szabályai

7.2.1.1 Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és internet böngésző biztonsági beállításai is.

7.2.1.2 Tilos a szervezeti egység vezetője, az üzemeltetés, valamint az informatikai biztonsági vezető jóváhagyása nélkül az intézeti munkához szorosan nem kapcsolódó internetes szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

7.2.1.3 Tilos az intézeti elektronikus információs rendszerek használata az intézeti értékekkel összhangban nem álló célokra (pl. fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, illegális kereskedelmi tevékenységre, internetes, illetve szerencsejátékokra, illetve bármilyen jogellenes tevékenységre).

7.2.1.4 Az internetről csak hivatali célból lehet fájlokat letölteni. Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása.

7.2.1.5 Tilos a felhasználóknak a hivatali e-mail-címüket nem hivatalos minőségben használni (pl. regisztráció letöltési weboldalakra, online játék oldalakra, közösségi oldalakra, nem munkához köthető szolgáltatások igénybevételére stb.).

7.2.1.6 Az internetes oldalak elérése monitorozásra és naplózásra kerül, a munkával összefüggésbe nem hozható oldalak elérhetőségét a munkáltató jogosult korlátozni a kormányzati informatikai szolgáltató útján.

7.2.1.7 A hivatali e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer egy figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a levelezési lehetőség.

7.2.1.8 Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

7.2.1.9 A felhasználók alapértelmezésben a levelezés során csak a saját postafiókjukat tudják kezelni, másokét nem látják, közös postafiókok elérése a szervezeti egység vezetője írásos indoklása mellett állítható be a kormányzati informatikai szolgáltató által.

7.2.1.10 Zavaró, félreinformáló levelek, spamek küldése, jogtalan megrendelések elindítása tilos.

7.2.1.11 Ismeretlen helyről származó e-mailt megnyitni nem szabad, mert maga a levél vagy annak csatolmánya kártékony kóddal, vírussal, illetve visszaélésre alkalmas tartalommal rendelkezhet, ezért az ilyen elektronikus leveleket csatolmányként a cert@im.gov.hu e-mail-címre történő küldést követően törölni kell.

8 Vírusvédelem

8.1 A vírusvédelem alkalmazásának előírásai

8.1.1 Az illetékes üzemeltető a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások, valamint a teljes internet és elektronikus levélforgalom folyamatos ellenőrzésére. A felhasználó számára a védelmi rendszer bárminemű megkerülése szigorúan tiltott. Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

8.1.2 Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

8.1.3 Ha a vírus helye nem lokalizálható, az illetékes üzemeltető jogosult a hálózat egyes funkcióit vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

8.2 Teendők vírusgyanú esetén

8.2.1 Vírusgyanú esetén a felhasználó – a hivatalvezető egyidejű tájékoztatása mellett – az IM IBV számára köteles azonnal jelezni azt a 2. függelék szerinti formanyomtatvány felhasználásával. Az IM IBV a kormányzati informatikai szolgáltató Ügyfélszolgálata felé a bejelentéssel kapcsolatos szükség szerinti intézkedéseket megteszi.

9 Az informatikai eszközök fizikai védelme

9.1 Számítógép használatának előírásai

9.1.1 A munkaállomást és a perifériákat a napi munkavégzés befejezésekor ki kell kapcsolni. Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (pl. hálózati nyomtatók, monitorok). Az elektronikus információs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

9.2 „Üres asztal – üres képernyő" politika

9.2.1 Az „üres asztal – üres képernyő" politika megvalósítása az alábbiakat jelenti:

9.2.1.1 a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel ez nem biztosítható, akkor sötétítő függöny használatával);

9.2.1.2 a felhasználó a munkaállomását zárolni köteles (a Ctrl+Alt+Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

9.2.1.3 6 órát meghaladó eltávozás esetén a munkaállomását ki kell kapcsolni;

9.2.1.4 bekapcsolva felejtett számítógép esetén a bejelentkezett felhasználó profiljának védelme érdekében jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

9.2.1.5 a munkafázis végeztével ki kell jelentkezni az alkalmazásokból;

9.2.1.6 a felhasználóknak az elektronikus információs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik.

9.3 Mobil elektronikus információs eszközök védelme

9.3.1 Az asztali munkaállomásokra vonatkozó előírásokon kívül a mobil elektronikus információs eszközök védelme érdekében az alábbi szabályokat kell betartani:

9.3.1.1 a mechanikai és használati sérülések elkerülése érdekében követni kell az eszköz használatához kapott útmutatót;

9.3.1.2 a cserélhető kártyák behelyezésénél és eltávolításánál szintén a használati utasítást kell követni;

9.3.1.3 a mobilitás és a kis méret miatt a mobil elektronikus információs eszközöket védeni kell a lopás ellen, azokat nem szabad őrizetlenül hagyni közösségi járműben, gépjárműben vagy olyan helyen, illetve helyiségben, ahol idegen személy hozzáférhet.

9.3.2 A mobil elektronikus információs eszközök eltűnése esetén

9.3.2.1 az eszköz eltűnését a lehető leggyorsabban – előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban – jelenteni kell a közvetlen munkahelyi vezetőnek és a szolgálati út betartásával az informatikai biztonsági vezetőnek a további szervezeti intézkedések megtétele céljából, valamint tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű érzékeny információt;

9.3.2.2 értesíteni kell a kormányzati informatikai szolgáltató Ügyfélszolgálatát a levelezésre is használt, munkaeszközként kiadott mobil elektronikus információs eszköz esetén a levelező rendszer online felületén az adott eszközre történő szinkronizálásnak a lehető leghamarabb történő tiltása érdekében;

9.3.2.3 amennyiben a körülmények más eljárást nem tesznek lehetővé, értesíteni kell a rendőrséget, és az üggyel kapcsolatban keletkezett valamennyi rendőrségi iratot meg kell őrizni, és az intézet részére a lehető leghamarabb át kell adni.

Biztonsági események és sérülékenységek – Felhasználói bejelentésének rögzítése

Az érintett elektronikus információs rendszer:

A tapasztalt biztonsági esemény megnevezése:

Az esemény tapasztalásának dátuma: ____ év ____ hó ____ nap

Az esemény bejelentésének dátuma: ____ év ____ hó ____ nap

Bejelentő neve:

Bejelentő szervezeti egysége:

Az esemény pontos leírása:

A bejelentés rögzítésének dátuma: ____ év ____ hó ____ nap

HOZZÁFÉRÉS-ELLENŐRZÉS

1 A szervezeti hozzáférés-ellenőrzés követelményei

1.1 Az információkhoz és a folyamatokhoz történő hozzáférést a működési és biztonsági követelményeknek megfelelően kell szabályozni, az intézet elektronikus információs rendszereire irányadó biztonsági besorolás alapján.

2 A hozzáférés-ellenőrzés alapszabályai

2.1 Csak jóváhagyott hozzáférés-védelmi megoldások alkalmazhatóak. A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:

2.1.1 A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

2.1.2 Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.

2.1.3 Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.

2.1.4 Az összeférhetetlenségi szabályokat figyelembe kell venni.

2.1.5 Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

2.1.6 Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságok adminisztrációját az elérhető legteljesebb módon, a felmerülő kockázatok figyelembevételével automatizálni kell.

2.1.7 A papíralapú jogosultság nyilvántartás csak és kizárólag azon esetekben alkalmazható, amelyekben informatikailag támogatott megoldás költséghatékonyan nem valósítható meg.

2.1.8 Minden egyes elektronikus információs rendszerhez csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani és felfüggeszteni, illetve visszavonni.

2.1.9 Az éles üzemű elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal csak fennálló feladataikkal arányosan, a megrendelő szakterület és az IBV által megadott keretek között rendelkezhetnek.

3 A felhasználói hozzáférések kezelése

3.1 Meg kell akadályozni az elektronikus információs rendszerekhez történő illetéktelen hozzáféréseket. Szabályozott eljárással ellenőrizni kell a hozzáférési jogok kiadását az elektronikus információs rendszerekhez és a szolgáltatásokhoz.

3.2 A felhasználói hozzáférések kialakítása

3.2.1 A felhasználók nyilvántartásba vételi szabályainak és a követendő eljárásrend kidolgozásakor az illetékes üzemeltetőnek a következőket kell figyelembe venni:

3.2.1.1 A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.

3.2.1.2 A csoportos felhasználó azonosítók használatát tiltani kell.

3.2.1.3 A felhasználói hozzáférési jogosultságokat a szervezeti egység legalább főosztályvezető szintű vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:

3.2.1.4 a felhasználó munkakörét és az azzal kapcsolatos feladatait;

3.2.1.5 a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságengedélyezés elvét;

3.2.1.6 a felhasználó jogviszonyát;

3.2.1.7 a felhasználó munkahelyét.

3.2.2 A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell:

3.2.2.1 a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;

3.2.2.2 annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;

3.2.2.3 azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;

3.2.2.4 annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;

3.2.2.5 az érintett önálló szervezeti egység vezetőjének (főosztályvezető) aláírását.

3.2.3 A jogosultságigénylés dokumentációját az igényelt és a beállított jogosultságok egyeztetése céljából az üzemeltető tárolja.

3.2.4 A kiosztott felhasználói jogosultságokat az informatikai biztonsági vezető szükség esetén ellenőrizheti.

3.3 Privilegizált felhasználó-kezelés

3.3.1 A felhasználói jogosultságok kiadási folyamatánál szigorúbban kell kezelni a privilegizált jogokat biztosító adminisztrátori jogok megadását. Az elektronikus információs rendszereknél a jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:

3.3.1.1 pontosan meg kell határozni azokat a rendszerelemeket – pl. operációs rendszereket, adatbázis-kezelő rendszert, valamint az alkalmazásokat – és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni;

3.3.1.2 az adminisztrátori jogosultságokat a „feltétlenül szükséges" és az „eseményenkénti" használat elve alapján kell kiadni;

3.3.1.3 az IM elektronikus információs szakrendszerek tekintetében a rendszeradminisztrátori jogosultságot (privilegizált felhasználó) kizárólag az illetékes üzemeltetési terület informatikai üzemeltetésért felelős vezetője engedélyezhet írásban, az IBV egyidejű tájékoztatása mellett;

3.3.1.4 felhasználói munkaállomás üzemeltetés esetén az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá, a részükre biztosított adminisztrátori jogosultság birtokában csak a felhasználó külön engedélyével és jelenlétében, kifejezetten a hiba elhárítása érdekében vagy a felhasználói igény kielégítése érdekében férhetnek hozzá a felhasználók által kezelt információkhoz.

3.4 Jelszókezelő rendszer

3.4.1 A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszerrel szembeni alapvető elvárás, hogy hatékonyan és interaktívan biztosítsa a megfelelő színvonalú jelszavak használatát.

3.4.2 Az intézet elektronikus információs rendszerei elérésére szolgáló jelszókezelő rendszer

3.4.2.1 tegye lehetővé a felhasználók számára jelszavuk megváltoztatását, és kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

3.4.2.2 beíráskor vizuálisan értelmezhető módon ne jelenítse meg a jelszavakat a képernyőn;

3.4.2.3 a jelszó állományokat titkosítva tárolja;

3.4.2.4 kényszerítse ki a megfelelő minőségű jelszavak használatát;

3.4.2.5 ahol a felhasználók maguk adják meg jelszavukat, kényszerítse ki meghatározott időközönként a jelszóváltoztatást;

3.4.2.6 tiltsa meg a korábban használt jelszavak ismételt felhasználását;

3.4.2.7 korlátozott számú sikertelen próbálkozás után a bejelentkezés lehetőségét tiltsa le, amelyet követően a bejelentkezés ezt követően rendszer/szervezeti adminisztrátori beavatkozás segítségével valósulhat meg újra;

3.4.2.8 változtassa meg a szállító alapértelmezett jelszavát a szoftver telepítését, illetve éles üzembe helyezését követően.

4. függelék a 4/2020. (VI. 29.) sz. hivatalvezetői utasításhoz

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND

1 Az eljárásrend célja, hatálya, alapelvek

1.1 Az eljárásrend célja az intézeten belül az elektronikus információbiztonsági kockázatkezelési eljárás szabályozása, mely a kockázati tényezők meghatározására, azok értékelésére, a kockázatokra adott válaszreakciókra, a kockázatok felülvizsgálatára, a kockázatkezeléssel összefüggő munkafolyamatokra, az ezzel összefüggő feladatokat ellátók hatáskörére, felelősségére és a dokumentálás rendjére terjed ki. A szabályzat rendelkezései arra irányulnak, hogy a 41/2015. (VII. 15.) BM rendelet 4. mellékletében foglalt vonatkozó követelmények – az intézeti szervezet sajátosságainak figyelembevételével – teljesüljenek.

2 Értelmező rendelkezések, a kockázat

2.1 Értelmező rendelkezések:

2.1.1 Elektronikus információbiztonsági kockázatkezelési rendszer: olyan folyamatalapú kockázatkezelési rendszer, amely a szervezet minden ilyen irányú tevékenységére kiterjed, egységes módszertan és eljárások alkalmazásával, a szervezet célkitűzéseinek és értékeinek figyelembevételével biztosítja a szervezet elektronikus információbiztonsági kockázatainak teljes körű azonosítását, azok meghatározott kritériumok szerinti értékelését, valamint a kockázatok kezelésére vonatkozó intézkedési terv elkészítését és az abban foglaltak nyomon követését;

2.1.2 Korrupció: a Büntető Törvénykönyvről szóló 2012. évi C. törvény XXVII. Fejezetén belüli tényállások.

2.2 Az elektronikus információbiztonsági kockázat fogalma, típusai

2.2.1 A kockázat szűkebb értelemben az intézet elektronikus információbiztonsági céljait veszélyeztető tényező.

2.2.2 A kockázat tágabb értelemben egy a jövőben valamilyen valószínűséggel bekövetkező esemény, tevékenység vagy annak elmulasztása, amelyek bekövetkezése negatív hatással lehet az intézet által kitűzött elektronikus információbiztonsági célok elérésére.

2.2.3 A kockázat ok-okozati megközelítésből lehet:

2.2.3.1 véletlenszerű esemény;

2.2.3.2 hiányos ismeret vagy információ;

2.2.3.3 az ellenőrzés hiánya, illetve gyengesége.

2.2.4 A kockázat típusa szerint lehet:

2.2.4.1 Külső környezeti (stratégiára ható) kockázat az, amely hosszabb távon és esetleg időközönként módosuló formában, valamint tartalommal hat, és független az intézet működésétől. A külső környezeti kockázatot az intézet befolyásolni nem képes, de bekövetkezésére a vezetés megfelelő stratégiával képes felkészülni, hatását mérsékelni, kivételes esetekben kiküszöbölni;

2.2.4.2 Belső (működési) kockázat az, amely az intézet működésének, tevékenységének, folyamatainak rövidtávon ható hozadéka, melynek kiküszöbölése vagy mérséklése a vezetéssel szemben támasztott követelmény;

2.2.4.3 Eredendő kockázat az intézet feladatkörével és működésével kapcsolatos olyan belső sajátosság, ami a környezeti hatások vagy az erőforrások elégtelensége miatt hibák előfordulásához vezethet, és ami önmagában az intézet által nem befolyásolható;

2.2.4.4 Kontrollkockázat az, amikor az intézet belső kontrollrendszere a nem megfelelő kialakítás, illetve működtetés miatt nem képes feltárni vagy megelőzni a hibákat, szabálytalanságokat;

2.2.4.5 Maradványkockázat a kockázatokra adott válaszintézkedés után fennmaradó kockázat;

2.2.4.6 Korrupciós kockázat a korrupció bekövetkezésének veszélye.

3 Kockázatelemzési módszertan

3.1 A kockázatelemzés alapelvei:

3.1.1 Az intézet infokommunikációs rendszereiben előállított, feldolgozott és tárolt adatok, illetve a futtatott alkalmazások, valamint az ezeket fenyegető veszélyek együttes fenyegetettség- és kockázatelemzését három szempont összevetésével kell elvégezni:

3.1.1.1 Az elektronikus információs rendszerek védelmi igényét a három alapfenyegetettség: a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából kell osztályozni. Az osztályozási szempontok az IBSZ 6. függelékében találhatók.

3.1.1.2 A tényleges fenyegetések számba vétele érdekében fel kell deríteni és értékelni kell az elektronikus információs rendszereket fenyegető veszélyeket és károkozó hatásukat.

3.1.1.3 Veszélyt csökkentő tényezőnek kell tekinteni azokat az eszközöket, intézkedéseket, amelyeket az intézet alkalmaz a fenyegető veszélyek kivédésére. Vizsgálni kell a védelmi intézkedések létezését, illetve a létező intézkedések megfelelőségét, erősségét.

3.1.2 A 3.1.1.1–3.1.1.3. alpontokban foglaltak együttes figyelembevételével meg kell határozni a bekövetkezés valószínűségét, és ezekből következően az intézet vizsgált elektronikus információs rendszerei informatikai biztonsági kockázatának mértékét, majd ezek alapján elvégezni a biztonsági osztályba sorolást.

3.2 A kockázatelemzés módszertan lépései:

3.2.1 Kockázatok meghatározása;

3.2.2 A felmérés hatályába eső vagyonelemek és tulajdonosaik meghatározása;

3.2.3 Vagyonelemeket veszélyeztető fenyegetések meghatározása;

3.2.4 Fenyegetések által kihasználható sérülékenységek meghatározása;

3.2.5 A bizalmasság, sértetlenség, rendelkezésre állás elvesztéséből származtatható vagyonelemekre vonatkozó hatások meghatározása.

3.3 A kockázat felmérése:

3.3.1 A vagyonelemek bizalmasságának, sértetlenségének, rendelkezésre állásának elvesztéséből származtatható károk meghatározása.

3.3.2 A folyamatok és az adatok érzékenységét – védelmi igényét – meg kell határozni.

3.3.3 A vagyonelemek bizalmasságának, sértetlenségének, rendelkezésre állásának, elvesztési lehetőségének meghatározása.

3.3.4 Kockázatok kezelési lehetőségeinek meghatározása és elemzése.

3.3.5 A megfelelő kontrollok meghatározása.

4 Az elektronikus információbiztonsági kockázatkezelés végrehajtásának szabályai

4.1 Kockázatkezelési hatókör:

4.1.1 A hivatalvezető saját hatáskörben kezeli a kockázatot, vagy ha a kockázat kezelése meghaladja a hatáskörét, – a kockázat hatásának jelentőségétől függően – azonnal tájékoztatja az IM IBV-t a feltárt kockázat kezelésére vonatkozóan javasolt intézkedési tervről.

4.1.2 Az IM IBV a 4.1.1. alpontban foglaltak szerint javasolt intézkedési tervről szükség szerint egyeztetést folytat a hivatalvezetővel, majd azt előterjeszti az IM közigazgatási államtitkárnak.

4.1.3 A kockázatokra adott válaszlépések kidolgozásáért és végrehajtásáért felelős személyek részére az IM közigazgatási államtitkár biztosítja az elektronikus információbiztonsági kockázatkezeléssel összefüggő feladatok ellátásához szükséges feltételeket.

4.2 Az elektronikus információbiztonsági kockázatkezelés folyamata:

4.2.1 Az elektronikus információbiztonsági kockázatkezelés során az adott rendszer felhasználói minőségű munkatársai felmérik és megállapítják az intézet elektronikus információbiztonsági tevékenységében rejlő kockázatokat, mely felmérés eredményeként évente egységes elektronikus információbiztonsági kockázati leltárt készítenek, amely a szervezet vonatkozó céljait fenyegető valamennyi feltárt kockázatot tartalmazza. Ezen a leltáron belül szükséges azonosítani a különféle speciális kockázattípusokat, majd meg kell határozni az egyes kockázatokkal kapcsolatban szükséges intézkedéseket, valamint azok teljesítésének folyamatos monitoringját.

4.2.2 A kockázatok kezelését éves ciklusban kell megvalósítani. Az ütemezést úgy kell kialakítani, hogy a kockázatok értékelése legkésőbb tárgyév október 31-ig, az elektronikus információbiztonsági kockázatkezelési intézkedési terv tárgyév november 30-ig elkészüljön.

4.2.3 Az elektronikus információbiztonsági kockázatkezelési intézkedési tervet a hivatalvezető hagyja jóvá.

4.3 A kockázatkezelés elemei:

4.3.1 A kockázatok feltárása, azonosítása az intézet céljainak elérését veszélyeztető kockázatok számbavételével történik.

4.3.1.1 A működési folyamatokra ható, korábban még nem tapasztalt kockázatokat a végrehajtási szinten feladatot teljesítő munkatársak kötelesek feltárni, és haladéktalanul jelenteni a hivatalvezető, szükség szerint az IM IBV felé a 4.1.1. alpontban foglaltak szerint.

4.3.1.2 A kockázatot feltáró munkatársak jelzései alapján az intézet valamennyi érintett szervezeti egysége vezetőjének fel kell mérni azt, hogy mi jelenthet kockázatot az általa irányított, felügyelt területen. A feltárt kockázatot a 4.1.1. alpontban foglaltak szerint kell a hivatalvezető útján az IM IBV elé beterjeszteni.

4.3.1.3 A beazonosított kockázatokról és az azokkal kapcsolatban előírt intézkedésekről az intézet nyilvántartást vezet.

4.3.1.4 A kockázatelemzés és értékelés során a kockázatokat feltáró munkatársak a szervezeti elektronikus információbiztonsági célok elérését veszélyeztető kockázatokat azonosítják és értékelik a válaszlépések (intézkedések) meghatározása érdekében. A kockázatok elemzése az egyes kockázatok előfordulási valószínűségének és lehetséges hatásának becslését jelenti. A kockázatok minősítése a 4.3.1.4.1. alpontban szereplő értékelés útján, a vonatkozó célokra gyakorolt hatás és a bekövetkezési valószínűség becsült nagyságának egy háromfokozatú – alacsony, közepes, magas – skálán történő besorolásával valósul meg.

4.3.1.5 Az egyszerű, kvalitatív (minőségi) értékeléssel történő kockázatelemzés során az adatgazdák, illetve a szervezeti üzemeltető háromfokozatú mátrixban – magas, közepes vagy alacsony – határozza meg az egyes kockázatok minősítését annak hatása és bekövetkezési valószínűsége alapján.

Kockázati kritérium mátrix

Az intézetre gyakorolt hatás			
Magas	K	M	M
Közepes	A	K	M
Alacsony	A	A	K
	Alacsony	Közepes	Magas
	A bekövetkezés valószínűsége		

4.3.1.6 A beazonosított kockázatokat a munkatársak – szükség szerint a döntéshozatalra jogosult vezető döntésének kezdeményezésével – a tervezéstől a döntéshozatalon át a végrehajtásig bármely munkafolyamat során kezelhetik, ha az feladat- és hatáskörüket nem haladja meg. Az elektronikus információbiztonsági kockázatkezelés legeredményesebb eszköze a hatékony folyamatba épített ellenőrzés. A folyamatba épített ellenőrzés hatékonyságát támogatja az ellenőrzési nyomvonal kialakítása. Az ellenőrzési nyomvonal kiépítése alapján lehet a megfelelő kockázatelemzési tevékenységet ellátni. A kockázat kezelésének módját és eszközét (az alkalmazni kívánt kontrollt) minden egyes beazonosított kockázat esetében külön kell meghatározni.

5 A kockázatkezelés módjai és főbb lehetséges eszközei

5.1 A kockázatkezelés módjai

5.1.1 A kockázatos tevékenység megszüntetése

5.1.1.1 Az intézet ezt a módszert csak korlátozottan, alaptevékenységének ellátásánál nem, csak kiegészítő tevékenységeinek ellátásához alkalmazhatja.

5.1.2 A kockázat elviselése, elfogadása

5.1.2.1 Az intézet vezetése akkor dönthet ezen kockázatkezelési mód választása mellett, ha a kockázat hatásának kivédése, illetve mérséklése több erőforrást vesz igénybe, mint a kockázatos tevékenységből származó kár.

5.1.3 A kockázat megosztása

5.1.3.1 Kiemelt és releváns kockázat megosztási technika a kiszervezés: a különleges szakértelmet kívánó feladatot arra specializálódott személlyel vagy szervezettel végeztetik (pl. külső szoftverfejlesztő vagy üzemeltető igénybevétele) a megfelelő garanciális feltételek beépítésével.

5.1.4 A kockázati kitettség csökkentése:

5.1.4.1 a nem kívánt következménnyel járó kockázat realizálódása lehetőségének korlátozásával, így különösen a belső szabályzatok, ügyrendek kialakítása, ezek jogszabálynak, illetve közjogi szervezetszabályozó eszköznek megfelelő módosítása, a pontos feladatmeghatározás, a hatáskörök és feladatkörök szétválasztása, a belső kontrollok kialakítása, működtetése, valamint az információhoz és az informatikai rendszerekhez való hozzáférés rendszeres felülvizsgálata;

5.1.4.2 a már realizálódott kockázat következményeinek és hatásának mérséklésével, így különösen szervezeti átalakítások, tartós vagy átmeneti munkaerő átcsoportosítás, jogszabály-, illetve közjogi szervezetszabályozó eszköz módosításának kezdeményezése;

5.1.4.3 meghatározott elektronikus információbiztonsági szakmai követelmény elérése, így különösen oktatási és képzési feladatok teljesítése;

5.1.4.4 a nem kívánt esemény bekövetkezése okainak feltárását célzó – jövőbeni hasonló hiányosságok ismétlődésének megakadályozását szolgáló – utólagos vezetői ellenőrzések vagy belső ellenőri vizsgálatok útján valósítható meg.

5.1.5 Az adott kockázat kezelési módjának meghatározására, valamint az annak végrehajtásával kapcsolatos kezdeményező intézkedés megtételére az érintett adatgazda, illetve szervezeti üzemeltető köteles.

5.2 A monitoring (nyomon követés) során kell elvégezni:

5.2.1 a helyi körülményekre és sajátosságokra kialakított elektronikus információbiztonsági kockázatkezelési rendszer időközönkénti felülvizsgálatát abból a célból, hogy az alkalmazott kockázatkezelési módszerek megfelelően segítik-e az intézet működését és vonatkozó feladatának ellátását, amelynek keretében minden egyes kockázat minősítését az érintett adatgazdának, illetve a szervezeti üzemeltetőnek – szükség szerint egymással történő együttműködésben – évente legalább egyszer felül kell vizsgálnia, annak időpontját lehetőleg az adott kockázat válaszlépéseinek határidejéhez igazítva;

5.2.2 a nyomon követés – a kockázatkezelés során választott módtól és eszköztől függően – az intézkedési tervben foglalt, az elektronikus információbiztonsági kockázatkezelés végrehajtásához szükséges feladat felelős általi, határidőben történő végrehajtásának ellenőrzését az IBV által.

5.3 A korrupció és csalás, mint kiemelt kockázati tényezők kezelése:

5.3.1 Az intézeten belül kiemelt figyelmet kell fordítani a súlyosabb szervezeti integritást sértő események (csalás, korrupció) mint kiemelt kockázatok kezelésére. Az elektronikus információbiztonsági kockázatkezelés során a szándékosan elkövethető szervezeti integritást sértő események megelőzésére kell a fő hangsúlyt helyezni.

5.3.2 A szándékos szervezeti integritást sértő események körébe tartozik különösen a csalás, a sikkasztás, a partnerrel, ügyféllel való összejátszás, a hivatali visszaélés, a nyilvántartások tudatosan meghamisított vezetése.