MAGYAR FELSŐOKTATÁSI AKKR

M A B

MAGYAR FELSŐOKTATÁSI AKKREDITÁCIÓS BIZOTTSÁG

INFORMÁCIÓBIZTONSÁGI SZABÁLYZATA

A MAB

INFORMÁCIÓBIZTONSÁGI SZABÁLYZATA

(Jelen szabályzatot a MAB Testület a 2026/2/XIV sz. határozatával elfogadta)

2026

Tartalom

1. Preambulum

1) Az informatikai rendszerek üzemeltetése során számos kockázati tényezővel és veszélyhelyzettel kell számolni, előtérbe helyezve azt a tényt, hogy ezeket a veszélyforrásokat teljes mértékben nem lehet megszüntetni. A kockázatok csökkentésére a Magyar Felsőoktatási Akkreditációs Bizottság (a továbbiakban MAB) információs vagyonát kezelő felhasználóinak és a rendszer üzemeltetőinek egyaránt törekednie kell, a cél ezeknek az elfogadható mértékre történő leszorítása. A cél elérése érdekében a MAB a kockázati elemeket folyamatosan vizsgálja, és az adott helyzetnek megfelelően kezeli.
2) A szabályozás egyaránt lefedi az információk helytelen kezeléséből származó kár megelőzésére tett lépéseket, az informatikai események és incidensek kezelését, valamint egy incidens bekövetkezése esetén a kár minimalizálását, illetve mentesítését.
3) Az informatikai incidensek elkerülésének érdekében a cél a veszélyhelyzet elkerülése és annak kivédése, amit adminisztratív és technikai eszközök segítségével kívánunk elérni. A cél elérését informatikai védelmi eszközökkel, azok működési felügyeletével, és észlelő kontrollokkal biztosítjuk azért, hogy a káros hatást megelőzzük vagy minimalizáljuk. Az adminisztratív eszközök (szabályzások) leírják az adott helyzet esetén szükséges cselekvések sorozatát is.
4) Az informatikai rendszerek védelmére az arányosság elvének betartása mellett a legnagyobb mértékű technikai védelmet biztosítjuk. A humán oldalról érkező incidensek minimalizálására szabályzási és képzési lépéseket teszünk.

2. Az Információbiztonsági Szabályzat célja

1) A jelen Szabályzat (a továbbiakban IBSZ) célja, hogy a MAB által működtetett információs, azon belül informatikai rendszerekre vonatkozó biztonsági intézkedéseket szabályozza, meghatározza a számítástechnikai eszközök beszerzésének és használatának, az üzemeltetés, a fejlesztés és alkalmazás, valamint az adatkezelés folyamatának biztonsági szabályait, definiálja az informatikai szerepköröket, és előírja az egyes szereplők informatikai biztonságot érintő feladatait. A papíralapú ügykezelés biztonságára vonatkozó részletes szabályokat a MAB Iratkezelési Szabályzata tartalmazza.
2) Az IBSZ feladata, hogy a célok eléréséhez keretet adjon az informatikai rendszerekben és azon kívül kezelt adatok bizalmasságának, hitelességének és rendelkezésre állásának biztosítása érdekében. A szabályozás alapja a MAB folyamatainak, adatainak és az azt kezelő rendszereknek biztonsági besorolása. Az IBSZ strukturális alapját az MSZ ISO /IEC 27001:2014-es szabvány képezi.
3) Az IBSZ az alábbi fő feladatokat tűzi ki:
   a) A MAB informatikai rendszereinek biztonsági osztályba sorolása.
   b) A titok- és adatvagyon védelmére vonatkozó előírások betartása.
   c) A személyes adatok védelméhez fűződő jogok kellő védelme.
   d) Az üzemeltetett számítástechnikai eszközök, hardverek, szoftverek, hálózatok stb. rendeltetésszerű használata és megfelelő üzemeltetése.
   e) Az üzembiztonságot szolgáló műszaki fenntartási és karbantartási teendők elvégzése.

f) A számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő károk megelőzése, illetve minimális mértékűre való csökkentése.
g) Az adatállományok formai és tartalmi helyességének és épségének megőrzése.
h) Az alkalmazott szoftverek sértetlenségének, megbízható működésének biztosítása.
i) Az adatállományok biztonságos mentése.
j) A felhasznált és keletkezett írásos dokumentumok megfelelő kezelésének biztosítása.
k) A MAB a MAB Titkárság vezető beosztású, és az informatikai rendszerekkel összefüggő feladatokat ellátó dolgozói számára meghatározza a felelősségi körükbe tartozó informatikai rendszerekkel kapcsolatos adatvagyonát, valamint az azt kezelő informatikai rendszer védelmével, biztonságával és megbízható működésével kapcsolatos feladatokat, definiálja az ehhez kapcsolódó felelősségi- és hatásköröket.
l) Az informatikai rendszerekkel kapcsolatos jogosultság és a hozzáférés rendszerének meghatározása.
m) A célok elérése érdekében az e szabályzatban foglaltaknak az egyes rendszerelemek teljes életciklusa alatt működnie kell – a megtervezéstől a működtetésükön át a felszámolásukig.

4) A MAB Információbiztonsághoz kapcsolódó feladatait a MAB Titkárság látja el.

3. Az IBSZ-hez kapcsolódó egyéb dokumentumok:

a) MAB adatvédelmi szabályzat
b) Iratkezelési szabályzat
c) Elektronikus másolatkészítési szabályzat
d) Szabályzat a mesterséges intelligencia felelős használatáról a Magyar Felsőoktatási Akkreditációs Bizottságnál
e) Balesetvédelmi előírások
f) Tűzvédelmi előírások

4. Általános rendelkezések

1) Az IBSZ hatálya kiterjed a MAB Titkárság összes dolgozójára, a MAB Testület és a Kollégiumok, Munkacsoportok tagjaira, és minden olyan személyre, aki a MAB-bal olyan jogviszonyba kerül, mely során a MAB informatikai infrastruktúrát és adatvagyont, vagy annak valamilyen részét kezeli, vagy a MAB informatikai rendszerét használja.
2) Jelen szabályzat kiterjed minden olyan harmadik félre is, amely számára a MAB hozzáférést biztosít az adatvagyon részének vagy egészének kezelésére, illetve a MAB informatikai infrastruktúra használatára. A harmadik fél számára hozzáférés csak abban az esetben biztosítható, ha a felhasználni kívánt információs rendszer felelőse ahhoz írásban hozzájárul, az igénybe vevő a jelen szabályzatban foglaltak betartását elfogadja, illetve titoktartási nyilatkozatot tesz.

5. Az IT rendszerek és adatok biztonsági besorolása

A MAB által működtetett rendszereket az alábbi öt biztonsági szint valamelyikébe kell besorolni. A besorolás alapja a rendszer és adatai által kiszolgált folyamatok kritikussága, az adatok értéke, a rendszer és adatainak kiesése, illetve elvesztése esetén keletkező kárérték. Ugyancsak a besorolás alapját jelenti az adatok érzékenysége, különös tekintettel a személyes és a különleges jellegükre.

1) Az 5. biztonsági osztályba sorolandó rendszerek és adatok olyan, a MAB feladatainak ellátása szempontjából kritikus adatok és rendszerek azok, amelyekre sérülésük vagy kiesésük esetén az alábbiak valamelyike fennáll:

   a) Nagymennyiségű személyes vagy különleges adat kerülhet nyilvánosságra.
   b) A nemzeti adatvagyon körébe tartozó adatvagyon megsérülhet vagy illetéktelen kezekbe kerülhet.
   c) Súlyos bizalomvesztés jöhet létre a MAB-bal szemben.
   d) A MAB ügymenete szempontjából nagyértékű, nem nyilvános információ kerülhet illetéktelen felhasználásra vagy nyilvánosságra.

   A MAB esetében ezek a rendszerek:

   a. TIR
   b. TIR 2.0
   c. Microsoft 365
   d. Irattári állomány
   e. HR és gazdasági adatállomány

2) A 4-es biztonsági osztályba sorolandó rendszerek és adatok olyan, a MAB feladatainak ellátása szempontjából kritikus adatok és rendszerek, amelyek sérülése vagy kiesése esetén az alábbiak valamelyike fennáll:
   a) Nagymennyiségű személyes vagy különleges adat sérülhet vagy kerülhet nyilvánosságra.
   b) Különlegesen érzékeny folyamatokat kezelő információs rendszer vagy különlegesen érzékeny folyamathoz kapcsolódó adat jelentős mértékben sérülhet.
   c) A MAB ügymenete szempontjából nagyértékű, nem nyilvános információ kerülhet illetéktelen felhasználásra vagy nyilvánosságra.
   d) Bizalomvesztés következik be, vagy az adott szolgáltatási terület vezetésében személyi felelősségre vonást kell alkalmazni.

   A MAB esetében ezek az alábbi rendszerek:

   a. Iktatási rendszer.
   b. Informatikai hálózat.
   c. Mobiltelefonok.
   d. Központi levelező kiszolgálók.
   e. Központi tárhely kiszolgálók.

3) A 3-as biztonsági osztályba sorolandó rendszerek és adatok olyan, a MAB feladatainak ellátása szempontjából kritikus adatok és rendszerek, amelyekre sérülésük vagy kiesésük esetén az alábbiak valamelyike fennáll:
    a) Személyes vagy különleges adat sérülhet vagy kerülhet nyilvánosságra.
    b) A MAB ügymenete szempontjából érzékeny folyamat alapjául szolgáló rendszer vagy adat sérülhet.
    c) Bizalomvesztés állhat elő az adott rendszerrel, ennek következtében az azt működtető szervezeti egységgel szemben.
    d) A szervezeti szabályokban foglalt kötelezettségek ellátása veszélybe kerülhet.

    A MAB esetében ezek az alábbi rendszerek:

    a. Szerverek
    b. Notebookok

4) A 2-es biztonsági osztályba sorolandó rendszerek és adatok olyan, a MAB feladatainak ellátása szempontjából kritikus adatok és rendszerek azok, amelyekre sérülésük vagy kiesésük esetén az alábbiak valamelyike fennáll:
    a) Csak csekély mennyiségű személyes adat sérülése következhet be.
    b) Csak csekély értékű adat, vagy kis fontosságú információs rendszer sérülhet meg vagy eshet ki.

    A MAB esetében ezek az alábbi rendszerek:

    a. Asztali számítógépek

5) 1-es biztonsági osztályba kell sorolni azokat az informatikai rendszereket, amelyek sérülésekor csak jelentéktelen káresemény következik be. Az 1-es biztonsági osztályba sorolt rendszerek nem kezelhetnek számottevő mennyiségű személyes adatot. A rendszer sérülésekor nem következhet be bizalomvesztés, a probléma a MAB-on belül marad és saját hatáskörben meg is oldható. Az esetleg bekövetkező anyagi kár jelentéktelen.

6. Információbiztonsági alapelvek

1) Az IBSZ szempontjából biztonságos állapot az, amikor a MAB adatvagyona, az azt tároló, és a folyamatokat kiszolgáló rendszerek bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű és a biztonsági besorolásuknak megfelelő szinttel arányos és folyamatos.
2) A 3-as, 4-es és 5-ös biztonsági osztályba sorolt rendszerek által kezelt adatok és az arra alapuló rendszerek védelmét a bizalmasság, sértetlenség és a rendelkezésre állás szempontjából úgy kell megvalósítani, hogy az informatikai rendszer és környezetének védelme folyamatos, teljes körű, zárt és kockázatokkal arányos legyen, és megvalósuljon a zárt szabályozási ciklus az alábbiak szerint:
    a) A védelem *folyamatos*, ha a változó környezeti feltételek mellett is megszakítás nélkül látja el a funkcióit. A folyamatos védelem megvalósítását az informatikai rendszer teljes életciklusa alatt, a beszerzéstől az üzemelésből történő kivonásig biztosítani kell.

b) A védelem *teljes körű* abban az esetben, ha a védelmi intézkedések az informatikai rendszer összes elemére kiterjednek, beleértve az alkalmazott hálózati modellt, és bármely két végpont között működő eszközt. A védelmet a fizikai, logikai és adminisztratív területek mindegyikén érvényesíteni kell az alábbiak szerint:
   i. Minden információbiztonsági rendszerelemre vagy csoportra, ideértve a központi, köztes és végponti berendezéseket.
   ii. Az informatikai rendszer infrastrukturális környezetére.
   iii. A rendszer működésében résztvevő hardver elemekre.
   iv. Az operációs rendszerekre és a folyamatokat kiszolgáló rendszerekre.
   v. A kommunikációs rendszerre, kiemelten a számítógépes hálózati kapcsolatokra.
   vi. A rendszert és adatait tároló adathordozókra.
   vii. A rendszerhez kapcsolódó dokumentumokra.
   viii. A rendszer üzemeltetőire.
   ix. A rendszer adataihoz hozzáféréssel rendelkező adatfeldolgozókra.
   x. A rendszer működtetésében résztvevő külső partnerekre.

c) A védelem *zárt*, ha tervezése során minden szóba jöhető fenyegetést figyelembe vettek, és a védelem ezek mindegyikével szemben megvalósul.

d) A védelem *kockázatarányos* abban az esetben, ha hosszú időtartamra vetítve a védelem költségei arányosak a potenciális kárértékkel úgy, hogy a védelemi intézkedések eredményeként a kockázatok elviselhető mértékűre csökkennek. A cél az elviselhető kockázatvállalás mellett a minimális költségráfordítás.

7. Az informatikai biztonság alapterületei

1) Az információvédelem, amely a MAB adatvagyonának védelmét jelenti a *bizalmasság*, és a *sértetlenség* területén függetlenül attól, hogy az adatvagyon elemeit elektronikus, vagy más formában tárolják.
2) A megbízható működés, amely a MAB információs rendszereinek rendelkezésre állását és az elvárt funkcionalitás képességének fennállását jelenti.

8. A MAB információbiztonsági politikája

1) A MAB biztonsági politikája minden üzemeltető és felhasználó számára meghatározza azokat az elveket és szabályokat, amelyek a MAB adatvagyon, valamint az azt kezelő rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának kialakítása és fenntartása érdekében szükségesek.
2) A MAB biztonsági politikájának elsődleges célja az adatvagyon és az információs rendszer elemeinek védelmén keresztül a MAB működési folyamatainak fenntartása. A MAB ennek szellemében minden, az adatvagyon kezelésében részt vevő munkatársától elvárja, hogy annak szakszerű kezelését a tőle elvárható mértékben valósítsa meg. Az adatvagyon bármely elemének veszélyeztetése az azt kezelő kizárását eredményezheti az adott rendszerből vagy annak mértékétől függően a teljes informatikai rendszerből.
3) Minden területen törekedni kell az arányossági elv betartása mellett a kockázatok minimalizálására.
4) Az adatvagyon minden területére meg kell határozni a felelősségi köröket.

5) Az információbiztonsággal kapcsolatos felelősségi köröket úgy kell meghatározni, hogy azok az egyes üzemeltetői és adatkezelői feladatok ellátásához legyenek kötve.
6) Törekedni kell a jogszabályi kötelezettségek betartására, különös tekintettel a GDPR-ra, a Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényre.
7) Az információbiztonsági ismeretek átadása, valamint, az ahhoz szükséges erőforrások rendelkezésre állásának biztosítása az informatikai vezető feladata.

9. Az üzemeltető hatásköre

1) Minden, a MAB által működtetett informatikai rendszer esetében az IBSZ szerinti működtetés felelőssége az alábbiak valamelyike:
   a) A rendszer informatikai kiszolgáló elemeinek, ideértve a szerverek, munkaállomások, operációs rendszerek, kliens szoftverek működtetését, az elektronikus rendszerekben tárolt adatvagyon technikai értelemben vett védelmét, és az azt kiszolgáló rendszerek üzemeltetését a MAB titkárság látja el.
   b) A rendszer működtetését a MAB-bal vállalkozási vagy megbízási szerződésben álló, az adott rendszer működtetésével megbízott személy vagy szervezet is végezheti. Ebben az esetben az IBSZ hatálya rájuk, és alvállalkozóikra is kiterjed.
2) Minden, a MAB titkárság által működtetett központi informatikai rendszer esetében az abban tárolt adatok kezelésének felelőse az informatikai vezető. Az ő feladata az adatok hozzáférési körének, valamint a rendszer által megvalósított folyamatok személyi körének meghatározása, annak rendszeres áttekintése, és a változások átvezetése az adott rendszerben. Az 5-ös, 4-es és 3-as biztonsági osztályba sorolt rendszerek esetében a hozzáférések beállítását az informatikai munkatársak számára adott írásos vagy e-mailben történő utasítás alapján végzik. A megbízásnak tartalmaznia kell a hozzáférésre jogosított munkatárs nevét, a hozzáférési jogokat vagy szerepköröket, a hozzáférés időtartamát és a jogosultságok kezelésével kapcsolatos elvek leírását. A MAB-bal jogviszonyban nem álló személy esetében hozzáférés csak a MAB elnök engedélyével lehetséges abban az esetben, ha annak megadása elkerülhetetlen.
3) A hozzáférési kör szabályozása a MAB vezető feladata abban az esetben is, ha az adatokat nem elektronikus információs rendszerben tárolják.
4) Abban az esetben, ha az adott informatikai rendszer üzemeltetését külső személy vagy szervezet végzi, a MAB vezetője felelős azért, hogy vele szemben érvényesítse az IBSZ követelményeit. Ennek érdekében a szolgáltatási szerződésekben szerepeltetni kell a következőket:
   a) A külső személy vagy szervezet felelősségvállalását az szerződés tárgyát képező informatikai rendszereire vonatkozóan, ideértve a mindenkor hatályos törvényi szabályzások, és a MAB belső szabályzásainak betartását.
   b) A szolgáltató által vállalt szolgáltatási szint megállapodást (SLA). Ebben ki kell térni a pontos vállalási körre, annak minőségi kritériumaira és azok mérésére és esetleges szankcióira. A szolgáltatói szerződéseknek minden esetben ki kell térnie az információbiztonsági, titoktartási és adatbiztonsági kérdésekre is.

   A szolgáltatási szerződésben foglaltak betartásának ellenőrzése, valamint a szükséges intézkedések foganatosítása az informatikai vezető feladata és felelőssége.

10. A felhasználók felelőssége

1) A MAB informatikai rendszerének minden felhasználója köteles az IBSZ-ben foglaltak szerint használni az informatikai rendszert.
2) Minden személy csak a számára meghatározott jogosultságokkal léphet be az informatikai szolgáltatásokba, és ezen jogok mentén használhatja a rendszert. A jogosultság változását a MAB vezetőjénél kell kezdeményezni, aki jelen IBSZ-ben szabályozott módon gondoskodik a hozzáférési engedélyek beállításáról.
3) Tilos a jogosultsági hozzáférések átadása más személy részére, és tilos egy hozzáférést több személyhez hozzárendelni.
4) Amennyiben egy szolgáltatás kezelője, illetve felhasználója megállapítja, hogy valamely informatikai rendszerben a számára szükségesnél magasabb jogosultsági szint érhető el számára, ennek tényét jeleznie kell a MAB Titkárság informatikai feladatellátásra kijelölt munkatársai felé. A magasabb jogkör meglétének okát ki kell vizsgálni.
5) A szolgáltatás felhasználója teljes felelősséggel tartozik az adott szolgáltatás igénybevételekor vállalt kötelezettségei betartásáért.
6) A MAB adatvagyona, függetlenül attól, hogy azt információs rendszerben vagy más módon tárolja, a MAB tulajdona. Az információs rendszereket minden munkatárs köteles csak a munkakörének megfelelően, az adott rendszer kezelési utasításainak és a kapcsolódó utasításoknak megfelelően használni.
7) Az 5-ös, 4-es és 3-as biztonsági osztályba sorolt adatok, illetve az ebbe az osztályba sorolt rendszerekből származó adatok kizárólag a MAB infrastruktúrán tárolhatók. Ezek az adatok hordozható számítógépeken, adathordozókon történő rögzítésükkor csak titkosítva tárolhatók azért, hogy esetleges elvesztésük esetén az adatokhoz való hozzáférés elkerülhető legyen.
8) Külső adattárolási szolgáltatások (Google Drive, Dropbox és alternatíváik) nem vehetők igénybe, helyettük a MAB saját felhőszolgáltatását (OneDrive és SharePoint) kell használni. Nem vehetők igénybe olyan külső adattárolási szolgáltatók, amelyek a náluk elhelyezett adatokat saját céljukra felhasználhatják, ennek ellenőrzése a tárolást végző személy feladata. Egy külső adattárolási szolgáltatónál elhelyezett, a MAB tulajdonát képező adatot érintő incidens megvalósulása esetén a felelősség a kihelyezést elrendelő, illetve az azt végző munkatársat terheli.
9) Az információs rendszerek kezelői csak munkaköri feladatuk ellátásához, annak szükséges mértékéig, és a titoktartási kötelezettségük betartásával kezelhetnek adatokat.
10) Az informatikai rendszer erőforrásaival minden felhasználónak takarékoskodnia kell. Különösen ideértve a SharePoint és az e-mailek tárolására szolgáló tárhelyet (pl.: e-mailben a csatolmányok helyett a fájlok SharePoint-on történő megosztás linkje kerüljön elküldésre, a SharePoint központi tárterületre csak a véglegesített munkaanyagok kerülhetnek fel, a személyes OneDrive-on kell tárolni a még nem véglegesített munkaanyagokat).
11) Az IBSZ előírásait abban az esetben is be kell tartani, amikor a felhasználók a MAB-ot valamely szakmai szervezetben képviselik.
12) A MAB bármely informatikai rendszerének felhasználója, vagy az adatvagyon valamely részének kezelője számára 2026. április 1-jétől kötelező információbiztonsági ismeretekkel rendelkeznie. Az újonnan belépő munkatársak számára a munkafolyamat

megkezdése előtt, de legkésőbb az első munkahéten, az egyéb kötelező oktatásokkal (tűzvédelmi, balesetvédelmi stb.) egyidőben meg kell történnie.

13) Amennyiben a felhasználó a magatartásával veszélyezteti az informatikai adatvagyont, az informatikai infrastruktúrát és az ezeken alapuló működési folyamatokat, az üzemeltető intézkedhet a szolgáltatásból történő kizárásról és jogainak visszavonásáról.
14) Az IBSZ előírásainak szándékos megsértése esetén a vonatkozó jogszabályoknak és a MAB előírásainak megfelelően szankcionálható.

11. A MAB Titkárságon belüli informatikai feladatok és felelősség

1) A MAB információbiztonsági vezetője az informatikai vezető és a jogi igazgató a feladatok szakmai megosztása mellett.
2) A MAB információbiztonsági szabályzását, az Információbiztonsági Szabályzatának készítését, felülvizsgálatát és aktualizálását az informatikai vezető és a jogi igazgató a feladatok szakmai megosztása mellett együttműködve végzi.
3) A MAB Titkárság informatikai feladatellátása körében ellátja az IBSZ-ben foglaltak betartásának ellenőrzését és incidens esetén lépéseket tesz annak kivizsgálására, az azt kiváltó okok megszüntetésére, a további incidensek bekövetkezésének megakadályozására, és a normál működés helyreállítására.
4) A MAB Titkárság informatikai feladatellátása körében fogja össze, koordinálja és üzemeltet minden, a MAB tulajdonában levő informatikai eszközt és szolgáltatást.
5) A MAB Titkárság informatikai feladatellátása körében koordinálja a szoftverek beszerzéseit és végzi azok nyilvántartását.
6) A MAB Titkárság informatikai feladatellátása körében engedélyezi az új informatikai elemek üzembe állítását. Ennek megadása során megvizsgálja az adott elem összeegyeztethetőségét a meglevő informatikai rendszerekkel, különös tekintettel az információbiztonsági megfelelőségre. Amennyiben az adott rendszerben ilyen irányú hiányosságot tár fel, az üzembe helyezést az informatikai vezető elutasítja, ebben az esetben az eszközt tilos üzembe helyezni.
7) Az informatikusok kérésre szakmai segítséget nyújtanak a megkötni kívánt szerződések informatikai tartalmának és paramétereinek kialakításában.
8) Az informatikai rendszerek IBSZ szerinti megfelelőségének vizsgálatát, az ezekkel kapcsolatos tanácsadást az informatikai vezető, illetve az általa kijelölt munkatársak végzik.
9) Az informatikai vezető felelős a kapcsolattartásért az IBSZ-hez kötődő szervezetekkel (pl. KIFÜ, HUNGARNET Egyesület). A tagsági és a kapcsolattartási kérdésekben a MAB elnöke dönt az informatikai vezető javaslata alapján, a MAB érdekeinek a figyelembevételével.

12. Az IBSZ-ben foglaltak megszegésének szankciói

1) Amennyiben az IBSZ az adott folyamat felelőseként az illetékes feladatokért felelős vezetőt határozza meg, aki a keletkezett kárért köteles helytállni.

2) A felhasználókat a szabályzatban foglaltak alapján az alábbi szankciók sújthatják:
    a) A szolgáltatás részleges felfüggesztése vagy az abból történő kizárás, melyről az informatikai vezető javaslata alapján a MAB elnök dönt.
    b) A felelősség megállapítása és az okozott kár megtérítése.
3) A szolgáltatásokat igénybe vevők szankcionálása csak abban az esetben történhet meg, ha az adott rendszer üzemeltetője dokumentálja a szankció elrendelését szükségessé tevő eseményt vagy incidenst, vagy a MAB Titkárság informatikai feladatellátása körében észlelte azt.
4) A MAB-bal polgári jogi megbízási jogviszonyban állók esetén a felelősségi és a kártérítési kérdésekben a polgári jog szabályai alapján kell eljárni.

13. Környezeti és fizikai biztonság

1) Fizikai biztonsági határvédelem. Az 5-ös biztonsági osztályba sorolt rendszerek kritikus komponensei, különösen a szerverek, tároló alrendszerek, routerek és kábelrendezők csak az erre a célra külön kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségben működtethetők.
2) Az 5-ös biztonsági osztályba tartozó rendszerek komponenseit tartalmazó helyiségekbe belépési jogosultságot a MAB elnöke adhat saját dolgozók vagy szerződéses partnerek számára. A belépési jogosultság nem ruházható át más személyre. Jogosulatlan személy belépéséért a felelősség a hozzáférést átadó személyt terheli.
3) A MAB informatikai rendszerelemeiről csak az informatikai vezető hozzájárulásával adható ki információ. Különösen tiltott az informatikai rendszerről bármilyen információ közzététele nyilvános, illetve közösségi oldalalakon.
4) Az irodák, szobák és egyéb létesítmények fizikai biztonsága.
    a) A MAB minden területén elvárt a „tiszta asztal, tiszta tábla, tiszta képernyő” elvének betartása. Ennek értelmében minden számítógép esetében gondoskodni kell a számítógép zárolásáról abban az esetben, ha a kezelője nem tudja a gépet a felügyelete alatt tartani. A használt operációs rendszerekben lehetőség szerint be kell kapcsolni az automatikus zárolási funkciót. Iratokat csak a szükséges ideig szabad látható helyen hagyni. A nyomtató, másoló berendezésekben nem szabad iratokat hagyni. A munka végeztével a számítógépet ki kell kapcsolni, és minden iratot zárható irodabútorokban kell tárolni.
    b) Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános védelmi területek használati módjával. Különleges vagy védett adatot tartalmazó informatikai eszközök, adathordozók csak az informatikai helyiségben helyezhetők el.
    c) Az informatikai célú helyiségek kialakításáról és átalakításáról az informatikai vezető dönt.
5) Külső környezeti károk elleni védelem.
    a) Az 5. biztonsági osztályú informatikai rendszerelemek kritikus fizikai komponensei csak a hatályos jogszabályozásnak megfelelő tűz- és villámvédelmi rendszerrel ellátott helyiségekben üzemeltethetők. Talajszinten, vagy az alatt működő helyiségek, irattárak esetében az ár- és belvízvédelmi szempontoknak is meg kell felelni.
    b) Egyedi esetekben az illetékes feladatokért felelős vezető egyéb előírásokat is tehet.

c) A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszereknek tartalmazniuk kell olyan kapcsolót, amely tűz esetén lehetővé teszi a biztonságos oltás végzését.
d) Az informatikai helyiség esetében biztosítani kell azt a hűtési kapacitást, amellyel az ott termelt felesleges hőmennyiség elvezetése megoldható.
e) Minden helyiség esetén biztosítani kell azt az erősáramú ellátó kapacitást, amellyel az ott működő informatikai eszközök elektromos betáplálása túlterhelésmentesen elvégezhető

6) Munkavégzés. Az 5-ös biztonsági osztályú rendszerek komponenseit tartalmazó helyiségekben minden, nem a MAB Titkárság informatikai feladatellátása kijelölt munkatársai által folytatott munkavégzést, ami az informatikai rendszereket, vagy azok működését veszélyezteti, csak előzetes egyeztetés után szabad elkezdeni. Az egyeztetést a munkát ellátó harmadik fél, és az informatikai vezető, vagy megbízottja végzi. A helyiség gépészeti elemeit veszélyeztető munkálatok csak az azt üzemeltető féllel történő előzetes egyeztetés és jóváhagyás után végezhetők. A szolgáltatás kiesésével járó tervezett munkavégzésekről a MAB Titkárság minden érintett munkatársát legalább 2 nappal korábban értesíteni kell.
7) Az 5-ös biztonsági osztályú rendszerek komponenseit tartalmazó helyiségekben mindenfajta szállítási tevékenység csak egy belépésre jogosult MAB Titkárság munkatársának felügyelete mellett alkalmazható.
8) Minden, az informatikai helyiségbe, illetve kábelrendezőkbe kerülő új rendszerelem elhelyezését előzetesen az informatikai vezetőnek jóvá kell hagynia. A jóváhagyás elutasítható abban az esetben, ha a helyiség nem rendelkezik a szükséges szabad hellyel, tápellátási vagy hűtési kapacitással.
9) A MAB Titkárság irodáiban elhelyezett informatikai kábelezési területeket, ideértve a kábelcsatornákat, alagutakat a MAB Titkárság informatikai feladatellátása kijelölt munkatársai felügyelik. Ezért azokban munkát végezni, a megközelítésüket korlátozni csak az informatikai vezető jóváhagyásával lehet.
10) A MAB Titkárság informatikai eszközeinek karbantartása.
    a) A MAB Titkárság informatikai feladatellátása kijelölt munkatársaknak minden informatikai komponenst kötelesek felmérni, azok karbantartási igényét meghatározni, azok karbantartási ciklusát az előírt időben betartani azt.
    b) A karbantartások során a felmerült sérülékenységeket ki kell küszöbölni, a karbantartásokat úgy kell elvégezni, hogy annak során ne merüljenek fel újabb sérülékenységek. A karbantartások lebonyolításáért MAB Titkárság informatikai feladatellátása kijelölt munkatársai a felelősek.
11) A MAB Titkárság székhelyén kívül használt eszközökkel kapcsolatos szabályok.
    a) A MAB Titkárság székhelyéről informatikai eszközt kivinni engedélyezett otthoni munkavégzés, vagy kiküldetés alapján lehet. Az eszközök mozgatását átadás-átvételi dokumentummal kell kísérni.
    b) A kivitel során vagy annak következményeként bekövetkező károkért, különös tekintettel az adatvagyonban, adatbiztonságban keletkezettekre, a kivitelt végző személy a felelős, amennyiben a kár számára felróható okból keletkezett. Az 5-ös, 4-es és 3-as biztonsági osztályú adatokat amennyiben az elkerülhető, nem szabad lemásolni, hanem az adott rendszert kell használni. Amennyiben az adatok másolása elkerülhetetlen, azokat kizárólag titkosított formában szabad a MAB Titkárság területéről kivinni. Az adatok kivitelét az illetékes feladatokért felelős vezetőnek engedélyeznie kell.

12) A már nem használt vagy meghibásodott adathordozók adattartalmát oly módon kell megsemmisíteni, hogy a tartalom ne legyen helyreállítható. Amennyiben az eszköz meghibásodott, az adathordozót a MAB Titkárság informatikai feladatellátása kijelölt munkatársai részére kell átadni, hogy az adathordozók szakszerű megsemmisítését elvégezhessék.
13) A papír alapú információk kifürkészésének elkerülésére a szükségtelenné vált iratok megsemmisítését úgy kell elvégezni, hogy azok tartalma illetéktelenek számára ne legyen megismerhető, lehetőség szerint iratmegsemmisítő gépet kell használni. Különösen tilos ezeket megsemmisítés nélkül hulladéktárolókba helyezni. A papír alapú dokumentumok információbiztonságával kapcsolatos további szabályokat a MAB Iratkezelési Szabályzata tartalmazza.
14) Az informatikai eszközöket a MAB Titkárság informatikai feladatellátása kijelölt munkatársai közreműködésével kell selejtezni. Az eljárás során megállapítást nyer a selejtezés indokoltsága, és szükséges esetben az adattartalom szakszerű eltávolítása. Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adathordozóit a selejtezés után fizikailag meg kell semmisíteni. A folyamat felelőse az informatikai vezető.

14. Fejlesztési és támogatási feladatok

1) A 4-es és az 5-ös biztonsági szintű fejlesztési feladatokat csak az eredeti rendszertől elkülönülten szabad végezni.
2) Amennyiben a fejlesztési feladatok ellátásához elengedhetetlen a védett adatokhoz történő hozzáférés, a fejlesztési rendszert az eredetivel megegyező biztonsági szintűnek kell minősíteni, és a hozzáférési jogosultságok nem haladhatják meg az eredeti rendszerben életben levőket.
3) A MAB Titkárság saját fejlesztésű, vagy ajándékba kapott szoftver csak funkcionális teszt után állítható üzembe.
4) Minden, a szolgáltatási felületen vagy funkciókészletében megváltozott szoftver esetében a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség nem csak az alkalmazások, hanem az azt futtató környezetek (webszerverek, adatbáziskezelők stb.) esetében is fennáll, de csak a használt funkciókra kell kiterjednie. A tesztek eredményét jegyzőkönyvben kell rögzíteni.

15. Üzemeltetés menedzsment

1) Új informatikai rendszer üzembe helyezése.
    a) A MAB Titkárság szolgáltatási igényének a MAB Titkárság informatikai feladatellátása kijelölt munkatársai csak abban az esetben tesznek eleget, amennyiben az abban foglaltak megfelelnek az IBSZ-nek. A MAB Titkárság informatikai feladatellátása kijelölt munkatársai a szolgáltatási igényt vagy saját szolgáltatásaival, vagy az igénylő az illetékes feladatokért felelős vezetővel történt egyeztetés után az igénylő által kívánt szoftverrel oldja meg.
    b) Amennyiben a MAB Titkárság új szoftver üzembe helyezését tervezi, annak biztonsági besorolását már a tervezési fázisban el kell végezni, és az üzemeltetés szabályait ennek megfelelően kell kialakítani.
2) Amennyiben MAB Titkárság új szoftvert kíván üzembe helyezni a MAB infrastruktúráján, a szoftvernek meg kell felelnie az IBSZ követelményeinek és a jogszabályi elvárásoknak, különös tekintettel a GDPR-ra. A megfelelőségről a szoftver

fejlesztőjének kell nyilatkoznia, amelyet a MAB Titkárság informatikai feladatellátása kijelölt munkatársa ellenőriz. A MAB Titkárság a megfelelőség hiányából adódó esetleges kárt a szoftver eladója felé hárítja át.

3) Kriptográfiai alapelvek
    a) Az informatikai rendszer minden pontján, ahol az a kockázattal arányosan megoldható, kriptográfiai megoldásokat kell alkalmazni.
    b) A kriptográfiai megoldások nem hagyhatók el az egyes rendszerekbe történő bejelentkezés, és az adatok forgalmazását végző csatornák esetén.
    c) Az információs rendszerek nem tartalmazhatnak kis erőforrás igényű eljárással dekódolható jelszavakat.
4) Jogkövető magatartás
    a) Tilos a MAB Titkárság tulajdonát képező bármely informatikai eszköz vagy szolgáltatás jogsértő tevékenység során történő felhasználása, ideértve a jogszerűtlen szoftver használatot, különösen az azok terjesztésében történő közreműködést.
5) Kártékony szoftverek.
    a) Azon rendszerek esetében, amelyekben kártékony kódok előfordulhatnak, a detektálásukra és elhárításukra szolgáló szoftvert kell telepíteni. A szoftver pontos típusát az informatikai vezető határozza meg, ettől eltérni nem lehet. Különösen tilos bármilyen, a védelmi szoftvert nem tartalmazó informatikai berendezést a MAB Titkárság informatikai hálózathoz kapcsolni.
    b) A felhasználó nem használhatja saját tulajdonú eszközét és adattároló berendezéseit a MAB Titkárság informatikai infrastruktúráján. A saját tulajdonú adathordozó MAB Titkárság informatikai rendszerhez történő csatlakoztatása következtében keletkezett kárért a csatlakoztatást végző személy a felelős.
6) Frissítések.
    a) A MAB Titkárság minden információs rendszerelemére telepíteni kell az operációs rendszer és az általuk működtetett rendszerek frissítéseit.
    b) A publikált sérülékenységek elleni védelem megvalósítása az adott rendszer üzemeltetését végzők feladata és felelőssége. A bizalmasságot, hitelességet vagy rendelkezésre állást közvetlenül fenyegető publikált sérülékenységekkel szembeni védekező intézkedés a publikációt követően a lehető legrövidebb időn belül hajtandó végre.
7) A MAB Titkárság hordozható számítógépet biztosít a munkatársai számára.
8) Az személyes használatra átadott, a MAB Titkárság tulajdonát képező számítógép indokolt esetben, de kizárólag az átvevő által magáncélra is igénybe vehető. Magáncélú használat esetén a magánjellegű adatokat a gépen tárolt egyéb adatoktól jól elkülönülten, egy kifejezetten erre a célra szolgáló, „Személyes_adatok” elnevezésű könyvtárból kiindulva kell tartani, más helyen tilos a személyes adatok tárolása. Az informatikai munkatársak ebben a könyvtárban semmilyen karbantartási munkát nem végezhetnek, annak tartalmát nem tekinthetik meg és azt nem menthetik. A magáncélú használat és a személyes adatok tárolása nem akadályozhatja a feladatok ellátását. A számítógép leadásakor a „Személyes_adatok” mappát a gép használójának kell törölnie.
9) A MAB Titkárság tulajdonát képező számítógépen kizárólag jogtiszta szoftverek futtathatók, különösen tilos bármilyen illegális forrásból származó, vagy feltört program futtatása, illegális tartalom letöltése. A magáncélú használatból kizárt a játékprogramok futtatása.
10) Amennyiben a MAB Titkárság egy munkatárs számára hordozható számítógépet biztosít, ezt a gépet kell használnia minden egyéb céges feladat ellátásához.

11) A MAB Titkárság tulajdonában álló eszközök biztonságáról minden munkatársnak gondoskodnia kell. A MAB Titkárság tulajdonában álló eszközben keletkezett hiba, vagy kár bekövetkezését a lehető legrövidebb időn belül jelezni kell az informatikai vezető felé. A hiba javítását kizárólag a szerződésekben vagy a garanciajegyen szereplő szerviz partner végezheti.
12) Amennyiben a MAB Titkárság tulajdonában álló informatikai eszközt ellopják, a MAB vezetőjének, vagy az eszköz használójának feljelentést kell tennie. A feljelentés jegyzőkönyvében foglaltak alapján a MAB Titkárság állapítja meg a kár mértékét és a munkatárs felelősségének mértékét.
13) A MAB Titkárság által kiadott e-mail címek nem használhatók magáncélú levelezésre.
14) Mentési eljárások.
    a) Minden 5-ös és 4-es biztonsági osztályba sorolt információs rendszer üzemeltetési leírásának tartalmaznia kell az adott rendszer és adatainak mentési eljárását, kitérve a mentési gyakoriságra, a mentés metódusára, a mentésért felelős személy meghatározására, a mentés ellenőrzésének periódusára és gyakoriságára, illetve az ellenőrzésért felelős személy meghatározására. A MAB üzemeltetésében levő, 5-ös biztonsági szintre sorolt rendszerek esetében off-site mentések tárolása is kötelező, a mentések tárolási rendjének alapkövetelménye a rendszer üzemeltetésétől távoli tárolás, illetve az őrzés biztonsága. A keletkező off-site mentések meglétét és olvashatóságát évente egyszer ellenőrizni, az ellenőrzés tényét dokumentálni kell.
    b) A 4-es és az alatti biztonsági szintű rendszerek esetében az on-site mentések is elfogadhatók, amennyiben azok fizikai elhelyezkedése az azokat működtető rendszer komponensektől különböző épületben helyezkedik el.
    c) A mentési rendet minden esetben úgy kell megtervezni és kialakítani, hogy a rendszer működőképessége bármelyik komponensének kiesése vagy adatainak elvesztése után esetén elfogadható mértékű adatvesztés mellett helyreállítható legyen. A helyreállítási tervben szerepelnie kell a teljes rendszer helyreállítási leírásának is. A mentési és helyreállítási terveket a rendszerek verzióváltásakor, de legalább évente egyszer felül kell vizsgálni, melynek felelőse az adott rendszerért felelős informatikai munkatárs.
    d) Az alkalmazások és informatikai eszközök (ideértve a switcheket, routereket is) konfigurációját annak minden módosítása után menteni kell.
    e) Az 5-ös biztonsági osztályú rendszerek adatait minden munkanap végén teljes egészében menteni kell. A mentési módnak biztosítania kell, hogy azok egy teszt rendszerbe visszatölthetők legyenek. A 4-es és az alatti biztonsági osztályba tartozó rendszerek adatai esetében a növekményes mentési eljárások is választhatók.
    f) Minden 5-ös biztonsági osztályba sorolt rendszer esetén legalább évente egyszer visszaállítási tesztet kell végezni, melynek célja annak ellenőrzése, hogy a mentésekből az eredeti rendszer és adatai biztosan visszaállíthatók-e. A visszaállítási tesztet az eredetivel funkcionálisan megegyező környezetben kell elvégezni. A visszaállítási tesztet és annak eredményét írásban dokumentálni kell.
    g) A munkaállomásokon lehetőség szerint csak minimális mennyiségű adatot szabad tárolni. A munkavégzés során keletkező adatokat a MAB Titkárság által biztosított felhőszolgáltatásban kell tárolni (OneDrive, SharePoint)
    h) A mentés elvégzésének felelőssége a munkaállomást használó felhasználóé, a mentés elmulasztásából adódó kár a munkaállomást használó munkatárs

felelőssége. A mentést lehetővé tevő szoftver telepítését és működésének beállítását a MAB Titkárság informatikai feladatellátása kijelölt munkatársai végzik el.

15) Hálózatbiztonság menedzsmentje.
   a) A MAB teljes hálózati infrastruktúrája egységes koncepció és megvalósítási stratégia mentén kerül kiépítésre. Az irányelvek meghatározását a MAB Titkárság informatikai feladatellátása kijelölt munkatársai végzik, a kiépítést külső szolgáltató cég bevonásával valósul meg.
   b) A MAB egységes WiFi hálózatot üzemeltet. Különösen nagy biztonsági kockázatot jelent, ezért kifejezetten tilos WiFi végpont (router, AP) jóváhagyás nélküli üzembe állítása.
   c) A kommunikációs hálózathoz csak a MAB Titkárság informatikai feladatellátása kijelölt munkatársai által engedélyezett és jóváhagyott eszközt szabad kapcsolni.
   d) A MAB területén csak a MAB Titkárság informatikai feladatellátása kijelölt munkatársai által engedélyezett és jóváhagyott internet-hozzáférést szabad használni. Különösen nem megengedett a MAB informatikai hálózat bármilyen összekötése vagy megosztása bármilyen más hálózattal, ideértve a GSM szolgáltatáson alapuló mobiltelefonos kapcsolatot is.
   e) A MAB Titkárság informatikai feladatellátása kijelölt munkatársainak engedélye és felügyelete nélkül kifejezetten tiltott bármilyen külső hálózati kapcsolat belső hálózati szolgáltatásban végződtetése, pl. VPN szerver, vagy különféle tunnelek létrehozása.
   f) A nem használt hálózati végpontok hálózati kapcsolatát fel kell függeszteni.
   g) A MAB Titkárság informatikai feladatellátása kijelölt munkatársai üzemeltetik a MAB tűzfal rendszerét. A tűzfal alapértelmezés szerinti biztonsági beállítása a kapcsolatok tiltása. Az egyes szolgáltatások számára szükséges kommunikációs utakat az adott rendszer működési előírásainak megfelelően szabad megnyitni. A tűzfal újabb portjainak megnyitása kizárólag a munkavégzéshez szükséges szoftverek működésének érdekében végezhető el.
   h) A tűzfal beállításait rendszeresen felül kell vizsgálni, és a szükségtelenné vált kapcsolati utakat be kell zárni.

16) Médiakezelés.
   a) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adatainak mentéseit tartalmazó adathordozók jogvédelem alá eső adatokat, személyes adatokat tartalmazhatnak. Ezeknek az adathordozóknak a kezelésére ugyanazok a szabályok vonatkoznak, mint az adatokat eredetileg tároló rendszereszközökre.
   b) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adatainak mentéseit tartalmazó adathordozók az informatikai helyiségben lemez-, vagy páncélszekrényben kell tárolni. Az adathordozókról és azokhoz történő hozzáférésről a szekrényhez hozzáféréssel rendelkező személynek nyilvántartást kell vezetni.
   c) Az adathordozók mentésből történő kivonása és szakszerű megsemmisítése a MAB Titkárság informatikai feladatellátása kijelölt munkatársainak a feladata.

17) Szerviz tevékenységek.
   a) Minden informatikai eszköz szerviztevékenységre történő átadása előtt gondoskodni kell az adattartalom illetéktelen személy általi megismerésének megakadályozásáról.

18) Információcsere.

a) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerek adatain automatikus adatcserét megvalósító kapcsolatok és folyamatok létesítéséhez az informatikai vezetőnek és az adott rendszert üzemeltető illetékes feladatokért felelős vezetőnek az engedélye szükséges. A kapcsolat kérelmezésekor az üzemeltetőknek pontosan részletezniük kell az adatkezelés célját, az alkalmazott műszaki megoldást kiemelten az adatcsere biztonságát megvalósító műszaki megoldásokra.
b) Az adatcsere környezetét és technológiai megoldásait az adatcserét kezdeményező alkalmazás üzemeltetőjének dokumentálnia kell.

19) Monitorozás.
a) Az informatikai rendszer felügyeletére automatikus felügyeleti rendszert kell üzemeltetni.
b) A felügyeleti rendszer komponenseinek ki kell terjednie a szerverek, aktív hálózati elemek, menedzselhető nyomtató-másoló berendezések és minden, a rendszerbe beköthető informatikai berendezés állapotára és folyamatainak felügyeletére.

20) Archiválás.
a) A MAB Titkárság által kivezetésre került rendszereit, amennyiben azt az illetékes feladatokért felelős vezető elrendeli, archiválni kell.
b) Az archív rendszerek biztonsági besorolását az azokban tárolt adatok jellege alapján a használatban levő rendszerekre vonatkozó szabályok szerint kell elvégezni.
c) Az archív rendszerekre ugyanazok a szabályok vonatkoznak, mint a használatban levőkre, különös tekintettel a hozzáférési jogosultságok meghatározására.
d) Az archivált rendszerekről már nem szükséges rendszeres biztonsági másolatot készíteni, de rendelkezni kell off-site mentéssel, amelyből szükség esetén az archivált rendszer helyreállítható.

16. Emberi erőforrások

1) A MAB információs rendszeréhez történő hozzáférés alapja a MAB elnökének az engedélye.
2) Új munkatárs felvétele esetén a munkatárs adatait a MAB Titkárság informatikai feladatellátása kijelölt munkatársainak fel kell vennie az M365 rendszerbe. Az ehhez szükséges adatokat a MAB Titkárság illetékes feladatokért felelős vezetője a felvételi döntés után küldi meg az informatikai vezető számára.
3) Az M365 rendszerben licenszel alapvetően csak a MAB Titkársággal kinevezéses jogviszonyban állók szerepelhetnek. Ideiglenes jogviszonyú munkatársak számára csak a jogviszony fennállásáig érvényes, csak az adott feladatkör ellátására alkalmas hozzáférés biztosítható. A hozzáférésnek a jogviszony lejártakor automatikusan meg kell szűnnie.
4) A MAB Titkárság dolgozói számára minden információs rendszerben csak azok a jogkörök biztosíthatók, amelyek a munkakörének ellátásához szükségesek. A munkakör megváltozását a MAB Titkárság illetékes feladatokért felelős vezetője írásban jelzi az informatikai vezető felé. Amennyiben MAB Titkárság illetékes feladatokért felelős vezetője a jogosultsági változás kérelmét elmulasztja, az ebből adódó következmények felelőssége őt terhelik.

5) Egy munkatárs jogviszonyának megszűnése esetén a hozzáféréseit meg kell szüntetni. A megszüntetés az erre szolgáló kilépési lap kitöltésével történik. A MAB Titkárság informatikai feladatellátása kijelölt munkatársai
a lap elfogadásával a kilépés határnapjával megszünteti az informatikai rendszerekhez adott hozzáféréseit, átveszi a munkatárs számára átadott informatikai eszközöket. A lejárt érvényességi idejű hozzáféréseket automatikusan tiltani kell.

   A jogviszony megszűnése után a munkatárs a MAB adatvagyonának semmilyen részének másolatával nem rendelkezhet. A titoktartási kötelezettség a jogviszony megszűnése után is fennáll.

17. Hozzáférés és jogosultságok szabályozása

1) Hozzáférési politika.
   a) Authentikáció. Minden, a MAB információs rendszerében tárolt adatot és szolgáltatást hozzáférési védelemmel kell ellátni. A hozzáféréseket személyre szólóan kell kialakítani. A hozzáféréseket csak az a személy használhatja, akinek azt kiadásra került. A hozzáférés történhet felhasználói névvel és jelszóval, valamint kétfaktoros authentikációval.
   b) Authorizáció. A hozzáférésekhez az egyes alrendszerekben szerepköröket, ennek hiányában objektum szintű jogosultságokat kell meghatározni. A szerepköröket és a jogosultságokat abban a legkisebb körben kell meghatározni és beállítani, hogy a felhasználó feladatköre még elvégezhető legyen. A minimális jogkör elve az illetékes feladatokért felelős vezetőire is érvényes, számukra sem állítható be a szerepkörükhöz nem szükséges jogkör. A rendszer üzemeltetését és a mentéseket készítő rendszer adminisztrátorok számára, amennyiben feladatuk másképp nem végezhető el, teljes hozzáférési jogosultságot kell adni.
   c) Hozzáférés nélkül az egyes rendszerekből kizárólag publikus adatok lehetnek kinyerhetők.
   d) A szerepköröket és a jogosultságokat évente egyszer felül kell vizsgálni. A felülvizsgálat eredményét a rendszert üzemeltető illetékes feladatokért felelős vezetőnek kell ellenőriznie és jóváhagynia.
2) A hozzáférési jelszavakat minden rendszerben egyirányú titkosítással kell tárolni. A MAB informatikai rendszerében nem működhet olyan komponens, amely jelszavakat olvasható formában, vagy elavult titkosítással kódol.
3) Amennyiben a MAB adatvagyonának titkosítása során felhasznált kódolási eljárás elavulttá válik, a kódolási eljárást le kell cserélni egy megbízható változatra.
4) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerekhez szükséges jelszavakat meghatározott időszakonként cserélni kell.
5) A MAB rendszereit úgy kell kialakítani, hogy azok ne tegyék lehetővé egyszerű jelszavak használatát.
6) Minden rendszerben korlátozni kell a sikertelen bejelentkezési kísérletek számát. A sikertelen bejelentkezési kísérleteket naplózni kell. A belépési kísérletekről az 5-ös, 4-es és 3-as biztonsági osztályú rendszerekben a naplózáson túl lehetőség szerint az automatikus felügyeleti rendszernek jelzést kell adnia az üzemeltető személyzet számára.

7) Az 5-ös, 4-es és 3-as biztonsági osztályú rendszerekhez hozzáféréssel rendelkező munkatársak részére az adott rendszer üzemeltetését végző illetékes feladatokért felelős vezetőnek fel kell hívnia a figyelmet az IBSZ-ben foglaltak betartására.
8) Távoli hozzáférés.
    a) Az 5-ös biztonsági osztályú rendszerekhez kizárólag a MAB belső hálózatából működtethetők hálózati kapcsolatok. Minden egyéb hozzáférési kísérlet informatikai incidensnek minősül, amelyet az informatikai üzemeltető személyzetnek detektálnia kell, és ki kell vizsgálnia.
    b) A MAB Titkárság a távmunka lehetőségének biztosítására VPN megoldáson alapuló távoli elérést biztosít a dolgozói számára. A VPN kapcsolati végpontok kiépítése és felügyelete a MAB Titkárság informatikai feladatellátásra kijelölt munkatárs feladatköre. Szigorúan tilos az informatikai vezető engedélye nélküli VPN kiszolgáló telepítése.
9) Operációs rendszer hozzáférés.
    a) Azokon a számítógépeken, melyekről 5-ös, 4-es és 3-as biztonsági osztályú rendszerekhez privilegizált felhasználóként történik hozzáférés, a felhasználók nem rendelkezhetnek teljes hozzáféréssel.
    b) A teljes jogú hozzáférést indokolt esetben az illetékes feladatokért felelős vezető által megbízott személy vagy a MAB Titkárság informatikai feladatellátásra kijelölt munkatársa birtokolja.

18. Megfelelőség

1) A mindenkori jogszabályi megfelelőség biztosítása a MAB Titkárság feladata.
2) Hatósági felszólításra a jogszabályban előírt adatokat a MAB Titkársága hatóság részére kiadja és amennyiben szükséges, az adott ügyben a hatóságokkal a jogszabályi előírás mértékékéig együttműködik.
3) Az információbiztonsági követelmények betartását és az információbiztonság tudatosság szintjének mérését a MAB Titkárság informatikai feladatellátásra kijelölt munkatársai penetrációs tesztekkel is végezheti.
4) Azon rendszerek esetében, amelyek üzemeltetése nem felel meg az IBSZ-ben foglaltaknak, egy esetleges incidens felelőssége az alkalmazás felhasználóját terheli.

19. Új információs rendszerek elfogadási eljárása

1) Új információs rendszer bevezetése előtt, már a tervezési fázisban egyeztetni kell a szolgáltatás üzemeltetőivel az alábbi szempontok alapján:
    a) Meg kell határozni a rendszer fejlesztőjét, üzemeltetőit és a rendszer életciklusát.
    b) Az üzemeltetést végzőknek jóvá kell hagyni a rendszer adatainak tárolásával és a biztonságos üzemeltetéssel kapcsolatos funkcióit és eljárásait. Amennyiben a biztonságos üzemeltetés nem valósítható meg, az üzemeltetők a rendszer működtetését megtagadhatják.
    c) Meg kell határozni és jóvá kell hagyni a rendszerekkel kapcsolatos támogatási feladatok, az azt ellátó személyek körét a rendszer teljes életciklusára vonatkozóan.

20. Információbiztonsági események menedzsmentje

1) A MAB információs rendszerével és az adatvagyonával kapcsolatos szokatlan, vagy a normál működéstől eltérő eseményeket be kell jelenteni a szolgáltatás üzemeltetőjének.
2) A MAB Titkárság kezelésében levő informatikai rendszer és adatvagyon esetében köteles kialakítani azokat a kommunikációs csatornákat, amelyeken incidens bejelentéseket fogad. Ezek a következők:
    a) E-mail: informatika@mab.hu
    b) Telefon: +36 70 519 7318
    c) Személyesen az informatikai feladatellátásra kijelölt munkatársak
3) Az informatikai rendszerekkel kapcsolatos biztonsági hiba észlelése vagy megismerése esetén azt be kell jelenteni az informatikai vezető felé.
4) A biztonsági hiba kihasználása a Btk-ba ütköző cselekmény, a MAB Titkárság ilyen esetekben jogi eljárást kezdeményez minden olyan esetben, amikor a hibát észlelő személy elmulasztja annak jelzését az üzemeltetők felé, vagy a biztonsági hibát nyilvánosságra hozza.
5) Biztonsági esemény bejelentésekor a bejelentőnek minden olyan birtokában levő adatot csatolnia kell, amely az esemény kezeléséhez szükséges lehet.
6) Tömeges érintettség esetében az üzemeltetőknek a normál kommunikációs csatornákon kell tájékoztatást nyújtaniuk.
7) A 4-es és 5-ös szintű rendszerek esetében üzletfolytonossági és incidenskezelési tervet kell készíteni.
8) Az incidensek bejelentését az üzemeltetők kötelesek súlyosságuk szerint besorolni és annak megfelelően az incidenskezelési eljárást megindítani és lefolytatni.

21. A MAB-on kívülre történő adatátadás

1) Adatok kiadása a 4-es és az 5-ös biztonsági szintbe sorolt adatvagyonból csak a MAB elnök engedélyével történhet, mely alól kivételt képeznek a törvényi kötelezettségek alapján történő adatszolgáltatások.
2) Személyes adatok kiadása csak az arra jogosultak által, a hatályos jogszabályoknak megfelelően, a GDPR ide vonatkozó előírásainak különös figyelembevételével, a belső szabályozás alapján történhet.
3) Az átadott adatok védelméért a hatályos jogszabályok alapján az átvevő fél felel.
4) Az adatszolgáltató az átadást megelőzően tájékoztatást kérhet az informatikai vezetőjétől adatvédelmi és információbiztonsági kérdésekben.

22. Az IBSZ felülvizsgálata

1) Jelen IBSZ felülvizsgálatára háromévente kerül sor. A következő esedékes felülvizsgálat időpontját a dokumentum lezárásakor kell meghatározni. Az IBSZ felülvizsgálatát emellett el kell végezni minden olyan esetben, amikor:
    a) azt érintő jogszabályi változás lép életbe, vagy az olyan technikai, műszaki, információbiztonsági változás történik, amely az IBSZ-módosítását igényli;
    b) új munkafolyamatok, szolgáltatások kerülnek bevezetésre vagy szűnnek meg;
    c) új, lényeges kockázati elem válik ismertté;
    d) biztonsági incidens elemzése utáni intézkedés bevezetése van szükség.

2) Az IBSZ-szel kapcsolatos véleményeket, változtatási igényeket az informatikai vezetőnél kell benyújtani. Az igénynek tartalmaznia kell a benyújtó adatait, a megváltoztatásra javasolt bekezdés(ek) számát, a javasolt új szövegrészt és annak indoklását.

Kelt: Budapest, 2026. február 26.

Dr. Szilágyi János Ede
a MAB elnöke