

**A Magyar Nemzeti Bank 11/2020. (X.20.) számú ajánlása
a pénzügyi szervezetek működésének fizikai biztonsági és humánkockázatkezelési feltételeiről**

I. Az ajánlás célja és hatálya

Az ajánlás célja a Magyar Nemzeti Bank (a továbbiakban: MNB) elvárásainak megfogalmazása a pénzügyi szervezetek működésének fizikai biztonsági és humánkockázatkezelési feltételeivel kapcsolatban, és ezzel a jogalkalmazás kiszámíthatóságának növelése, a vonatkozó jogszabályok egységes alkalmazásának elősegítése.

Az ajánlás összefoglalja azokat az eljárásokat, amelyeket a pénzügyi szervezeteknek a biztonságos működésük érdekében alkalmazni célszerű. Az MNB jelen ajánlás közzétételével biztosítja, hogy a felügyelt intézmények számára nyilvánosak legyenek a fizikai biztonsági és humánkockázatkezelési feltételekkel szemben támasztott felügyeleti elvárások.

Jelen ajánlás együttesen alkalmazandó az informatikai rendszer védelméről szóló 8/2020. (VI. 22.) MNB ajánlással, tekintettel arra, hogy ezek együttesen fedik le a fizikai és logikai biztonsági, valamint a humánkockázatkezelési követelményrendszert.

Jelen ajánlás címzettjei a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (a továbbiakban: Hpt.) hatálya alá tartozó hitelintézetek és pénzügyi vállalkozások, valamint a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (a továbbiakban: Bszt.) hatálya alá tartozó befektetési vállalkozások, ideértve az ezen típusú, az Európai Unió másik tagállamán vagy az Európai Gazdasági Térségről szóló megállapodásban részes más államon kívüli országban székhellyel rendelkező (harmadik országbeli) pénzügyi szervezetek magyarországi fióktelepét is (a továbbiakban együtt: pénzügyi szervezet). Az MNB javasolja továbbá az ajánlás alkalmazását a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 39. §-ában meghatározott jogszabályok hatálya alá tartozó más, pénz- és értékgorgalmat, fizikai biztonsági és humánkockázatkezelési belső előírásokat kialakító szervezetek és személyek számára is.

A pénzügyi szervezetek működése biztonsági feltételeinek kialakítását meghatározó és befolyásoló legfontosabb szabályozó eszközöket az ajánlás 1. számú melléklete tartalmazza.

Jelen ajánlás a jogszabályi rendelkezésekre teljeskörűen nem utal vissza az elvek és elvárások megfogalmazásakor, az ajánlás címzettjei a kapcsolódó jogszabályi előírásoknak való megfelelésre azonban továbbra is kötelesek.

Jelen ajánlás adatkezelési, adatvédelmi kérdésekben iránymutatást nem fogalmaz meg, a személyes adatok kezelése vonatkozásában semmilyen elvárást nem tartalmaz, és az abban foglalt követelmények semmilyen módon nem értelmezhetők személyes adatok kezelésére vonatkozó felhatalmazásnak. Az ajánlásban rögzített felügyeleti elvárások teljesítésével összefüggésben történő adatkezelés kizárólag a mindenkor hatályos adatvédelmi jogszabályi rendelkezések betartásával végezhető.

II. Értelmező rendelkezések

1. Jelen ajánlás alkalmazásában:

1.1. adat: tények, koncepciók vagy utasítások formalizált megjelenítése, beszéd vagy technikai eszközökkel történő közlés, értelmezés és feldolgozás számára;

1.2. bizalmasság: a titokvédelmi szempontból lényeges értékek, adatok védelme a jogosulatlan megismerés ellen;

1.3. biztonság: a pénzügyi szervezet zavartalan működéséhez, az adatok és a rendszerek bizalmasságának, sértetlenségének és megfelelő rendelkezésre állásának biztosításához szükséges elvi védelmi intézkedések meghatározása és azok technikai megoldásokkal történő kikényszerítése;

1.4. biztonsági incidens: minden olyan esemény, amely a fizikai biztonságra nézve potenciális fenyegetést jelent;

1.5. biztonsági kockázat: a fenyegetettség bekövetkezési valószínűségének és a bekövetkezéskor keletkező károknak a függvénye;

1.6. biztonsági szervezet (személy): a biztonsági tevékenység ellátására rendelt szervezet, szervezeti egység vagy az azt végző személy;

1.7. biztonsági tevékenység: a tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való gondoskodás, amely a pénzügyi szervezet saját tulajdonú eszközeinek, más fontos érdekeinek, értékeinek, valamint a kezelésében lévő idegen tulajdonú értékeknek, továbbá az alkalmazottak személyi tulajdonának és személyes biztonságának védelmét, illetve az ügyfeleket a pénzügyi szervezet területén veszélyeztető jogsértő magatartások megelőzését, felderítését, illetve folytatásának megakadályozását szolgálja és a biztonsági szabályzatban foglaltak végrehajtása (biztonsági feladatok ellátása) útján valósul meg;

1.8. elektronikai védelem: a biztonsági tevékenység végzését támogató elektronikus vagyonvédelmi rendszerek összessége;

1.9. elektronikus vagyonvédelmi rendszer: elektronikus jelző- és képi megfigyelőrendszer, ideértve a térfelügyeleti rendszert, az elektronikus beléptető rendszert, a betörésjelző rendszert, a távfelügyeleti rendszert, az adat- és informatikai védelemre irányuló biztonságtechnikai rendszert, továbbá az egyéb, jel és kép továbbítását vagy fény, illetve hang jelzését is lehetővé tevő elektronikus műszaki megoldást;

1.10. emberi erőforrás irányából felmerülő kockázatok: emberi mulasztásból vagy szándékos emberi tevékenységből származó fenyegetettségek bekövetkezési valószínűségének és a bekövetkezéskor keletkező károknak a függvénye;

1.11. értéktár: a trezor (páncélterem), ahol ilyen nincs, a munkatermekben elhelyezett, tűzzel és áttöréssel szemben ellenálló vagy a MABISZ által értéktárolásra alkalmasnak minősített páncélszekrények;

- 1.12. értéktárolás: az érték értéktárban, értéktároló eszközben történő tárolása nyitvatartási időben és azon kívül;
- 1.13. értéktároló eszköz: az értékek tárolására szolgáló eszközök, így különösen a páncélszekrények, épített trezorok, ATM-ek, értéktárolásra alkalmas multiszéfek;
- 1.14. értéktároló helyiség: az értéktároló eszközök elhelyezésére szolgáló helyiség;
- 1.15. humánkockázati incidens: emberi magatartás miatt bekövetkezett esemény (eseménysorozat), amely a pénzügyi szervezet vagy munkavállalóinak megítélésére, személyére, illetve tevékenységére közvetlen, vagy közvetett módon negatív hatással van, így különösen:
- külső és belső visszaélés,
 - életet, testi épséget, dologi, személyiségi, személyhez fűződő vagy szellemi alkotásokkal kapcsolatos jogokat, egyéb jelentős jogi tárgyat sértő vagy veszélyeztető jogellenes emberi magatartások,
 - pénzügyi szervezet működésével összefüggésben elkövetett bűncselekmények, szabálysértések;
- 1.16. információ: jelentéstartalommal bíró, értelmezett adat, mely felhasználója számára ismeretet hordoz és bizonytalanságot szüntet meg;
- 1.17. információbiztonsági-fizikai követelmények: az elektronikus és papír alapon tárolt információ biztonságát szolgáló fizikai védelmi intézkedések;
- 1.18. irányítási jogkörrel rendelkező vezető testület: a Hpt.-ben és a Bszt.-ben meghatározott fogalom;
- 1.19. kockázatarányos és hatékony védelem: a becsült és a bekövetkezett biztonsági incidensek által okozott, realizált vagyoni és nem vagyoni károk mértékéhez igazodó, a biztonsági incidensek megismétlődésének kockázatait is figyelembe vevő védelem;
- 1.20. letéti szolgáltatás, letétkezelés: a Hpt.-ben és a Bszt.-ben meghatározott fogalom;
- 1.21. létfontosságú rendszerelem: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 1. § f) pontja szerinti rendszerelem;
- 1.22. logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
- 1.23. mechanikai-fizikai védelem: a védendő objektumba történő illetéktelen behatolás elleni és az értékek fokozott védelmére szolgáló építészeti kialakítás, műszaki eszközök, valamint az információk és az értékek biztonságos tárolását szolgáló mechanikai berendezések alkalmazása;
- 1.24. rendelkezésre állás: az erőforrások folyamatos rendeltetésszerű biztosítása;
- 1.25. rendkívüli incidens: olyan biztonsági incidens, amely magában hordozza a pénzügyi szervezet rendeltetésszerű működésének, tevékenysége ellátásának akadályozását (például az ügyintézés

nyugalmának megzavarását vagy félelemkeltést), személyek életének, testi épségének veszélyeztetését, súlyos vagyoni kár vagy üzleti veszteség lehetőségét;

1.26. sértetlenség: értékek és adatok jogosulatlan megváltoztatása elleni védelme és forrásuk hitelességének biztosítása;

1.27. trezor, trezorhelyiség: olyan helyiség, amely értéktároló eszköz és értéktároló helyiség is egyben;

1.28. veszélyforrás: mindaz az esemény, cselekmény vagy mulasztás, amely biztonsági incidenst okozhat;

1.29. védendő helyiség: a pénzügyi szervezet minden olyan helyisége, ahol készpénzzel vagy értékpapírokkal, azok forgalomba hozatalával, átváltásával, tárolásával kapcsolatos műveleteket végeznek, továbbá minden olyan – a titokvédelem szempontjából fontos – helyiség, ahol bank-, üzleti, személyes, értékpapír-, biztosítási vagy pénztártitkot tartalmazó iratokat, információkat tárolnak, dolgoznak fel vagy használnak, valamint az, amit a pénzügyi szervezet a biztonsági szabályzatában ilyennek nyilvánít.

1.30. zóna-szintű elvek alapján megvalósuló kockázatarányos védelem: az eltérő funkcionalitású területek, helyiségek működésbeli sajátosságai alapján, a becsült és a bekövetkezett biztonsági incidensek által okozott, realizált vagyoni és nem vagyoni károk mértékéhez igazodó, a biztonsági incidensek megismétlődésének kockázatait is figyelembe vevő védelem.

III. A pénzügyi szervezet biztonságos működésének általános követelményei

2. A pénzügyi szervezet biztonságos működésének alapja a biztonságot támogató belső szabályozás és eljárások kialakítása, működtetése, valamint az azokhoz szükséges erőforrások fenntartása. A biztonságos működés megvalósítása érdekében az MNB elvárja, hogy a pénzügyi szervezet az ajánlásban rögzített biztonsági elvárásokat, valamint a működése során vállalt kockázat és a veszélyeztetettség mértékét figyelembe véve gondoskodjon az alábbiakról:

- a) rendszeres biztonsági kockázatértékelés végzése;
- b) biztonsági politika, biztonsági stratégia meghatározása;
- c) biztonsági szabályzat készítése;
- d) a 7-12. pontokban meghatározottakra figyelemmel biztonsági szervezet működtetése vagy biztonságért felelős személy alkalmazása;
- e) a rendszeres biztonsági kockázatértékelés eredményei alapján kockázatarányos és hatékony védelem kialakítása és fenntartása;
- f) a mechanikai-fizikai, az elektronikai, a logikai, az információbiztonsági-fizikai, továbbá az élőerős őrzés-védelemmel, a pénz- és értéktárolással, kezeléssel és szállítással összefüggő követelmények kockázatértékelésre alapuló, arányos meghatározása, alkalmazása és integrálása a jogszabályi kötelezettségekkel összhangban;
- g) a biztonsági követelményeket érintően a károk kockázat felmérése, megelőzése, valamint a későbbi kárvolumen csökkentése érdekében a Magyar Biztosítók Szövetsége (a

továbbiakban: MABISZ) „Betöréses lopás- és rablásbiztosítás technikai feltételei” című ajánlásában foglaltak, továbbá a vonatkozó nemzeti és európai uniós szabványok ajánlásainak figyelembevétele és kockázatarányos alkalmazása;

- h) a lehetséges károk csökkentése érdekében – elsősorban az értékezeléssel, szállítással és tárolással összefüggően – egyeztetés a kockázatvállalói oldal képviselőjével, valamint olyan megoldások alkalmazása, amellyel a káresemény bekövetkezési valószínűsége és vagyoni hatása csökkenthető;
 - i) az üzleti igényeihez igazodó szintű üzlet(ügy)menet-folytonosság, valamint a rendkívüli és katasztrófahelyzetek kezelési képességének biztosítása;
 - j) az emberi erőforrás biztonságát érintő és az emberi erőforrás irányából felmerülő kockázatok felmérése és kezelése;
 - k) a védelmi intézkedések eredményességének monitorozása; valamint
 - l) a felismert és a kezelt biztonsági incidensek, valamint a védelmi intézkedések rendszeres, két évente legalább egy alkalommal, írásban történő összegzése és értékelése, amely kiterjed a felismert és a kezelt biztonsági incidensek típusaira, a kockázatkezelő és csökkentő javaslatokra, valamint a kockázatarányos és hatékony védelem megvalósításához, fenntartásához szükséges beruházási, fejlesztési igényekre. Az értékelést az irányítási jogkörrel rendelkező vezető testület megtárgyalja és dönt a szükséges beruházási, fejlesztési igények elfogadásáról vagy elvetéséről. A pénzügyi szervezet gondoskodik az értékelés MNB részére történő megküldéséről.
3. Az MNB elvárja, hogy a pénzügyi szervezet a kockázatarányos és hatékony védelem tervezése, integrálása és működtetése során a jogszabályokban megfogalmazott követelmények betartása mellett a biztonságos működés érdekében tett fejlesztései során megismerje és a jogszabályokkal összhangban vegye figyelembe a hazai és nemzetközi jó gyakorlatokat, ajánlásokat, szabványokat, valamint egyéb védelmi képességeket fejlesztő biztonságirányítási elveket és módszereket.

IV. A biztonsági szabályzat

4. Az MNB elvárja, hogy a pénzügyi szervezet ezen ajánlás, a szakmai szövetségek által kiadott ajánlások, a hazai és nemzetközi jó gyakorlatok, valamint a vonatkozó biztosítási feltételek alapján a biztonsági politika, a biztonsági stratégia alapulvételével, részletes védelmi intézkedéseket felsoroló biztonsági szabályzatot készítsen. Elvárt, hogy a pénzügyi szervezet a szabályzatot a szabályozási rendszerben meghatározott eljárásrend alapján, dokumentáltan hatályba léptesse és a személyi hatálya alá tartozók számára megfelelően ismertesse, a szabályok megismerését dokumentálja, a hatályban lévő szabályzat elérhetőségét egyértelműen meghatározza.
5. Az MNB elvárja, hogy a biztonsági szabályzatban a pénzügyi szervezet a következőket állapítsa meg:

- a) a biztonsági szabályozás alá eső konkrét adat- és tárgykörök, a biztonsági osztályba sorolás alapján;
- b) a védendő helyiségek, valamint a védendő helyiségeket magukba foglaló épületek, épületrészek;
- c) a működés szempontjából stratégiai fontosságúnak ítélt épületek;
- d) a kijelölt létfontosságú rendszerelemek;
- e) a biztonsági védelem formáinak és eszközeinek kötelező alkalmazási rendjei a személyi és az objektumvédelemre, az élőerős őrzés-védelemre, a mechanikai-fizikai, az elektronikai, a logikai és az információbiztonsági-fizikai védelemre kiterjedően;
- f) a rendkívüli incidensek kezelésének, regisztrálásának (naplózás), kiértékelésének általános és speciális szabályai;
- g) a biztonsági szervezet szervezeti tagozódásai, a biztonsági szervezet, a biztonságért felelős személy, valamint a biztonsági szervezet vezetőjének részletes feladatai, hatásköri jogosítványai, kötelezettségei;
- h) a biztonsági tevékenységhez kapcsolódó feladatokat ellátó szervezet vagy személy irányítási jogkörrel rendelkező vezető testület felé történő beszámolásának gyakorisága;
- i) a vezetőknek és az alkalmazottaknak a biztonságért való általános és speciális felelősségi rendjei;
- j) a vezetőkre és az alkalmazottakra vonatkozó személyi védelmi intézkedések, kiemelve a fokozott veszélynek kitett munkakörök (személyek) védelmét;
- k) a munkavállalók biztonsági oktatásának rendjei; valamint
- l) a külső szolgáltató igénybevételének feltételei a biztonsági tevékenységhez kapcsolódó feladatok ellátására vonatkozóan.

V. A pénzügyi szervezet biztonságos működésének szervezeti feltételei

6. Az MNB elvárásai szerint a pénzügyi szervezet irányítási jogkörrel rendelkező vezető testülete a pénzügyi szervezet biztonságos működése érdekében ellátja az alábbi feladatokat:
 - a) a biztonságos működés feltételeire vonatkozó elvek alapján meghatározza a biztonsági politikát és stratégiát, valamint gondoskodik azok MNB részére történő megküldéséről;
 - b) jóváhagyja a biztonsági szabályzatot, valamint gondoskodik annak MNB részére történő megküldéséről;
 - c) gondoskodik a működésből eredő veszélyforrások felméréséről, továbbá – a biztonsági incidensek bekövetkezésének megelőzése érdekében – a védelem kialakításáról, a biztonság elérésére, illetve fenntartására vonatkozó szabályok kidolgozásáról, alkalmazásáról, a biztonsági követelmények betartásáról és az előírások betartásának ellenőrzéséről, valamint a rendkívüli incidensek kezelésére szolgáló terv elkészítéséről;
 - d) gondoskodik az adatok, információk és informatikai rendszerek bizalmas kezeléséről és az információk, valamint adatok sértetlenségének védelméről és rendelkezésre állásuk biztosításáról;

- e) a biztonsági kockázat csökkentése érdekében meghatározza a biztonsági szempontból fontosnak minősített munkakörök és ezen munkakörök betöltése szabályait, feltételeit;
 - f) biztosítja a biztonsági tevékenység végzéséhez szükséges személyi, tárgyi, anyagi feltételeket; továbbá
 - g) ellenőrzi a biztonsági szabályzatban foglaltak végrehajtását.
7. Az MNB elvárja, hogy a pénzügyi szervezetnél jelen ajánlás elvárásainak figyelembevételével jelöljenek ki egy olyan személyt, aki felelős a biztonsági tevékenységhez kapcsolódó feladatok ellátásának irányításáért, valamint azok jogszerűségének és eredményességének biztosításáért, ideértve a külső szolgáltató igénybevételével történő feladatellátás esetét is. Ez a személy lehet a biztonsági szervezet vezetője vagy a biztonságért felelős személy, ennek hiányában pedig az irányítási jogkörrel rendelkező vezető testület valamely tagja.
8. A 7. pont szerinti személy az irányítási feladatai tekintetében az MNB elvárása szerint az alábbiakat látja el:
- a) végzi a biztonsági szervezet szakmai irányítását;
 - b) irányítja a pénzügyi szervezet mechanikai-fizikai, elektronikai, élőerős védelmi rendszerei működését;
 - c) irányítja az informatikai rendszer védelmével kapcsolatos feladatok ellátását, amennyiben erre a pénzügyi szervezet irányítási jogkörrel rendelkező vezető testülete külön felelős vezetőt nem jelöl ki vagy külső szolgáltatót nem bíz meg;
 - d) értékeli, véleményezi a pénzügyi szervezet biztonságát érintő beruházási, fejlesztési terveket, gondoskodik az ahhoz szükséges pénzügyi eszközök igényének megfogalmazásáról, szakmai megalapozásáról, illetve azoknak az irányítási jogkörrel rendelkező vezető testület felé történő ismertetéséről; és
 - e) a biztonsági szabályzat tervezetét, illetve annak módosításait jóváhagyásra felterjeszti a pénzügyi szervezet irányítási jogkörrel rendelkező vezető testületének.
9. Az MNB elvárja, hogy a pénzügyi szervezet a biztonsági szabályzatban foglaltak végrehajtására a – 11-12. pontban foglaltak figyelembevételével – biztonsági szervezetet működtessen vagy biztonságért felelős személyt alkalmazzon.
10. A biztonsági szervezet (a biztonságért felelős személy):
- a) munkaszervezését, a szervezeti egység irányítását a pénzügyi szervezet a biztonsági szabályzatban foglaltaknak megfelelően végzi;
 - b) szervezeti tagozódását és feladatkörét a pénzügyi szervezet irányítási jogkörrel rendelkező vezető testülete, a Szervezeti és Működési Szabályzat, a biztonsági szabályzat, továbbá a biztonsági szervezeti egység munkaköri leírásai határozzák meg;
 - c) hatásköre, intézkedési jogköre kiterjed a pénzügyi szervezetre és az érdekkörébe tartozó objektumokra, személyekre.
11. A pénzügyi szervezet a biztonsági feladatok ellátása érdekében a vonatkozó szabályozó eszközök rendelkezéseinek és elvárásainak figyelembevételével külső szolgáltatót is igénybe

vehet, a hitelintézet azonban a biztonsági tevékenységhez kapcsolódó feladatok teljes körének ellátását nem alapozhatja csak külső szolgáltató igénybevételére.

12. Nem szükséges biztonsági szervezetet működtetni, illetve a 7. pontban hivatkozott személy mellett további biztonságért felelős személyt alkalmazni, amennyiben a hitelintézetén kívüli pénzügyi szervezet a biztonsági tevékenység teljes körének végzésére külső szolgáltatót bíz meg.
13. Az MNB elvárja, hogy a pénzügyi szervezet a biztonsági tevékenységet végző külső szolgáltató igénybevétele esetén mérlegelje, hogy az a pénzügyi szervezetre vonatkozó jogszabályok, ajánlások és az MNB által kiadott, nyilvános állásfoglalások¹ alapján kiszervezésnek minősül-e. Amennyiben a mérlegelés alapján a külső szolgáltató igénybevétele kiszervezésnek minősül, a pénzügyi szervezet az ajánlás 1. számú melléklete szerinti szabályozó eszközök rendelkezései, illetve elvárásai szerint jár el.
14. Amennyiben a biztonsági tevékenységet végző külső szolgáltató igénybevétele a fentiek szerinti mérlegelés alapján nem minősül kiszervezésnek, az MNB elvárja, hogy a pénzügyi szervezet a biztonsági tevékenységet végző külső szolgáltató igénybevétele során az alábbiak figyelembevételével járjon el:
 - a) a pénzügyi szervezet minden esetben felelős marad az általa alkalmazandó ágazati jogszabályokban meghatározott kötelezettségei teljesítéséért;
 - b) a pénzügyi szervezet felelős azért, hogy a külső szolgáltató a feladatot a vonatkozó előírásoknak és elvárásoknak megfelelően és a tőle elvárható gondossággal lássa el,
 - c) elvárt, hogy a pénzügyi szervezet egyértelműen rögzítse a külső szolgáltatóval összefüggő irányítási, belső kontroll, valamint nyilvántartási felelősségeket;
 - d) elvárt, hogy a pénzügyi szervezet a külső szolgáltatóval kötött hatályban lévő megállapodásairól mindenkor naprakész nyilvántartással rendelkezzen;
 - e) elvárt, hogy a pénzügyi szervezet biztosítsa, hogy a külső szolgáltató az ellátott feladatokkal arányos szakmai felelősségbiztosítással rendelkezik;
 - f) elvárt, hogy a pénzügyi szervezet folytassa le az igénybe venni kívánt külső szolgáltató átvilágítását, kitérve az alábbiak értékelésére:
 - fa) a tevékenységgel a külső szolgáltató megbízható-e (a külső szolgáltató adott tevékenységgel történő megbízása nem ütközik-e a külső szolgáltatóra vonatkozó jogszabályi előírásba vagy egyéb szabályozó eszköz által meghatározott korlátozó feltételbe, a külső szolgáltató rendelkezik-e a tevékenység végzéséhez szükséges hatósági engedéllyel, a külső szolgáltató megfelel-e a jogszabályi előírásoknak vagy egyéb szabályozó eszköz által előírt egyéb feltételeknek, valamint nincs-e egyéb objektív akadálya a külső szolgáltató igénybevételének, például nem áll-e felszámolás alatt, pénzügyi helyzete kielégítő-e);

¹ http://alk.mnb.hu/bal_menu/szabalyozo_eszkozok/allasfoglalasok

- fb) a külső szolgáltató megfelelő etikai sztenderdekkel és üzletvezetési gyakorlattal rendelkezik-e;
- fc) a pénzügyi szervezetnek a külső szolgáltatóval fennálló korábbi és jelenlegi kapcsolata, tapasztalatai;
- fd) a külső szolgáltatóval kapcsolatban felmerül-e érdekkonfliktus lehetősége, annak mik a lehetséges kezelési módjai; és
- fe) a külső szolgáltató megfelelő képességgel, kapacitással, elégséges erőforrással, személyi, tárgyi és biztonsági feltételekkel, megfelelő szervezeti felépítéssel rendelkezik-e a feladat hatékony, megbízható és magas szakmai színvonalú, az alkalmazandó jogszabályi és egyéb előírásoknak, elvárásoknak (például egyéb szabályozó eszközök, szokványok, szakmai és etikai sztenderdek) és a szolgáltatóval kötött megállapodásban meghatározott szolgáltatási szintnek megfelelő elvégzésére;
- g) elvárt, hogy a pénzügyi szervezet a külső szolgáltatóval kötendő megállapodás megkötése előtt felmérje annak működési kockázataira gyakorolt lehetséges hatását; valamint
- h) az MNB elvárja, hogy a pénzügyi szervezet a külső szolgáltatóval kötött írásbeli megállapodásában rögzítse:
 - ha) az ellátandó feladatokat és a felek viszonyát;
 - hb) a felek kötelezettségeit, ideértve különösen a külső szolgáltatónak a pénzügyi szervezet felé fennálló beszámolási kötelezettségét; és
 - hc) azt, hogy a pénzügyi szervezet folyamatosan nyomon követi a külső szolgáltató teljesítményét, valamint, hogy rendszeresen értékeli a külső szolgáltatóval kötött megállapodásait.

15. Külső szolgáltató igénybevétele esetén az MNB elvárja, hogy a pénzügyi szervezet időszakosan ellenőrizze a szolgáltató szolgáltatói megállapodásban is rögzített kötelezettségeit, különös tekintettel az alábbiakra:

- a) a külső szolgáltató által üzemeltetett, a pénzügyi szervezetet érintő berendezések folyamatos ellenőrzése, tesztelése, szolgáltatásfolytonossága, és
- b) amennyiben a pénzügyi szervezetet érintő dokumentációról a szolgáltató telephelyén, illetve eszközein is tárolt példány van, az információk bizalmosságának, sértetlenségének és rendelkezésre állásának biztosítása.

16. Az MNB elvárja, hogy amennyiben a biztonsági tevékenységhez kapcsolódó feladatok ellátása nem külső szolgáltató igénybevételelél valósul meg, a 7. pont szerinti biztonsági szervezet vezetője, illetve a biztonságért felelős személy a pénzügyi szervezettel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álljon.

17. Az MNB elvárja, hogy a biztonsági szervezet vezetőjének vagy a biztonságért felelős személynek a pénzügyi szervezet olyan személyt nevezzen ki, aki

- a) rendőrtiszti, katonai főiskolai vagy egyetemi végzettséggel, vagy egyéb egyetemi vagy főiskolai és felsőfokú, informatikai vagy biztonsági szakképesítést nyújtó végzettséggel rendelkezik, és

- b) legalább hároméves biztonsági, védelmi területen szerzett szakmai gyakorlattal rendelkezik, és
- c) büntetlen előéletű.

18. Az MNB elvárja, hogy a pénzügyi szervezet gondoskodjon arról, hogy a biztonsági tevékenységhez kapcsolódó feladatokat ellátó szervezet vagy személy szakmai tevékenysége során független legyen, megállapításai, tevékenysége, intézkedései során önállóan járjon el, továbbá az intézkedéseinek eredményességéről, a biztonságos működést támogató tervezésről rendszeresen, az irányítási jogkörrel rendelkező vezető testület döntése szerinti, a biztonsági szabályzatban rögzített gyakorisággal beszámoljon.

19. A biztonsági szervezet vagy a biztonságért felelős személy az MNB elvárásai szerint legalább a következő feladatokat látja el:

- a) részt vesz a pénzügyi szervezet biztonsági politikájának és stratégiájának kialakításában;
- b) elkészíti a pénzügyi szervezet biztonsági szabályzatának tervezetét;
- c) felülvizsgálja és aktualizálja a biztonsági szabályzatot minden szabályozási vagy alkalmazási környezetben vagy munkafolyamatban bekövetkező lényegi változás esetén, de legalább 2 évente;
- d) rendszeres biztonsági kockázatértékelést végez;
- e) tervezi, illetve megvalósítja a belső és külső biztonsági kockázatok azonosítására, csökkentésére és a biztonsági incidensek kezelésére vonatkozó intézkedéseket;
- f) a feltárt biztonsági kockázatok alapján megalkotja és kezeli a pénzügyi szervezet biztonsági-kockázati adatbázisát;
- g) kialakítja és vezeti a pénzügyi szervezet személyi és szervezeti infrastruktúráját érintő biztonsági események és incidensek kockázatértékelését, valamint regiszterét;
- h) folyamatosan azonosítja és kezeli a pénzügyi szervezet emberi erőforrásaiból származó, vagy személyüket érő kockázatokat;
- i) segíti és támogatja a visszaéléses típusú (belső, külső csalás, visszaélés, illetve egyéb, a vagyoni értékeket, üzleti célokat és jó hírnevet sértő vagy veszélyeztető) belső és külső emberi erőforrással megvalósított cselekmények megelőzését, vizsgálatát;
- j) belső biztonságtudatosító felkészítéseket, fórumokat szervez, végzi a vezető állású személyek és az alkalmazottak támadás vagy egyéb vészhelyzet esetén követendő magatartására vonatkozó oktatást;
- k) elemzéseket végez és javaslatokat tesz a megfelelő védelmi intézkedésekre és a biztonságos működéssel összefüggő szabályok megváltoztatására;
- l) a pénzügyi szervezet egyéb szervezeti egységei által tervezett vagy kiadott, a biztonsági szervezet hatáskörét érintő belső szabályzatokat, eljárásrendeket véleményezi, segíti biztonságsszakmai összehangolhatóságukat;
- m) végzi a védelmi intézkedések eredményességének folyamatos vizsgálatát;
- n) belső és külső fórumokon képviseli a pénzügyi szervezet biztonsági céljait, érdekeit;
- o) biztonságsszervezési, irányítási és vezetői feladatainak ellátása során rendszeres és eseti kapcsolatot tart a pénzügyi szervezet biztonságát támogató vagy annak megvalósításában

részt vevő belső és külső szervezetekkel, külső szolgáltatókkal, szervezeti egységek vezetőivel, munkavállalóival; továbbá

- p) eseti vagy rendszeres feladataihoz kötötten, valamint jogszabályokból, belső eljárásrendekből fakadó kötelezettsége szerint együttműködik a hatóságok képviselőivel.

VI. A biztonsági környezet azonosításának, kockázatelemzésének, valamint a fenntartható biztonsági szint működtetésének elemei

20. Az MNB elvárásai szerint a pénzügyi szervezet a biztonsági környezet azonosítása, kockázatelemzése, valamint a fenntartható biztonsági szint működtetése során legalább az alábbiakat figyelembe veszi:

- a) a védendő épület, épületrész alapterületének, határoló területeinek, illetve – amennyiben különálló ingatlannal rendelkezik – telekhatárait, lehetőség szerint a kapcsolódó közművek elhelyezkedését is tartalmazó tervrajzát, ennek hiányában helyszínrajzát;
- b) a közös használatú vagy közös falazattal rendelkező épületek, épületrészek, helyiségek felmérését;
- c) a határoló felületek építészeti sajátosságait figyelembe vevő kockázatokat, azok becslését (például áttörés és statikai képességek), lehetőség szerint statikai vagy építészeti dokumentációkkal alátámasztva;
- d) a biztonságos működéssel összefüggő kulcsfontosságú közműveket, azok vételezési helyét, a közművekhez történő csatlakozás és hozzáférés módját, jogosultjait, a közműveken szolgáltatást nyújtó gazdasági társaság alapvető adatait és elérhetőségét;
- e) a védendő épületben, épületrészben vagy a környezetében működtetett redundáns erőforrások (például generátor, aggregátor, másodlagos betáplálás) elhelyezkedését, az azok működését támogató szolgáltatók és karbantartók adatait, rendkívüli incidens során a biztonsági rendszerek működtetéséhez szükséges fenntarthatóságot, azaz időbeli, teljesítménybeli képesség adatait;
- f) a védendő épület, épületrész tűzvédelmi adottságait, előírásait, a már meglévő vagy kialakítandó beépített tűzjelző berendezés és önműködő indítású beépített tűzoltó berendezés típusát, elhelyezésének adatait, a működőképesség és törvényi kötelezettségek fenntartásához szükséges tanúsításokat, a kapcsolódó üzemeltetői, karbantartói adatokat;
- g) önműködő indítású beépített tűzoltó berendezés hiányában a tűzoltókészülékek elhelyezésének, működőképességének, valamint rendszeres és eseti karbantartásának adatait, tanúsításait;
- h) a védendő épület, épületrész környezetének közbiztonsági helyzetére utaló mérhető, megismerhető információkat, fokozott figyelemmel a vagyon és személy elleni cselekményekre; és
- i) a védendő épület, épületrész környezetében található, nagy forgalmú, közönség előtt is nyitott területeket, illetve a területek közbiztonsági helyzetére vonatkozóan megismerhető információkat.

21. Az MNB elvárja, hogy a pénzügyi szervezet biztonsági környezetének kockázatelemzése terjedjen ki az egyes kockázatokra alkalmazott kontrollok megfelelőségének vizsgálatára, adott esetben tesztelésére is.

VII. Élőerős őrzés-védelem

22. Az MNB elvárja, hogy a pénzügyi szervezet a jogszabályban nevesített esetekben, a biztonsági szabályzatban megállapított, a működés szempontjából stratégiai fontosságúnak ítélt épületben, valamint a kijelölt létfontosságú rendszerelemek tekintetében huszonnégy órás őrszolgálatot biztosítson.
23. Az MNB elvárja, hogy a pénzügyi szervezet üzleti célú létesítményeiben élőerős őrzés-védelmet biztosítson azon helyeken, melyek esetében az egyedi kockázatértékelés eredménye alapján az indokolt.
24. Az MNB célszerűnek tartja, hogy a pénzügyi szervezet a megfelelő élőerős őrzés-védelmet a létesítmény funkciója, a tárolt érték – beleértve a tárolt eszközökön elérhető vagy kezelt adatok értékét –, a napi ügyfél- és értékforgalom, valamint a létesítmények egyéb sajátosságainak figyelembevételével határozza meg.
25. Az MNB elvárja, hogy az őrszolgálatot külön jogszabályban² előírt szakvizsgálattal, szakképesítéssel rendelkező személy- és vagyonőr lássa el, valamint, hogy az őrzés-védelem biztosításával kapcsolatos szerződés írja elő a titoktartási kötelezettséget, az őrszolgálatot ellátók büntetlen előéletére vonatkozó kikötést.
26. A MNB jó gyakorlatnak tartja, ha a pénzügyi szervezet akkor is működtet őrszolgálatot, ha olyan vagyonvédelmi biztosítást kötött, amely biztosítja, hogy az okozott kár részben megtérül.
27. Az élőerős őrzés-védelem alkalmazásával összefüggésben az MNB elvárja, hogy a pénzügyi szervezet legalább az élőerős védelmi szolgáltatások és az azok során alkalmazott emberi erőforrások azonosítására alkalmas adatokat (név, munkakör, elhelyezési hely, elérhetőségek, rendkívüli incidens során a szállítás módja) nyilvántartsa, továbbá biztonságos és védett körülmények között, a jogszabályi követelményeknek megfelelően tárolja és kezelje.
28. Amennyiben az élőerős őrzés-védelem biztosítására külső szolgáltató igénybevételével kerül sor, az élőerős őrzés-védelemmel összefüggésben alkalmazott vállalkozás jogszabályokban meghatározott dokumentációinak megfelelőségét igazoló dokumentumait, a szolgáltatás hatályos szerződéseit, továbbá a gazdasági társaság érvényes felelősségbiztosításának dokumentációját vagy azok hiteles másolati példányát a megbízó telephelyén, az adatok tárolására szolgáló biztonsági tárolószekrényben elkülönítetten ajánlott tárolni. Ezen

² Különösen a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény, valamint a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról szóló 22/2006. (IV. 25.) BM rendelet.

dokumentumok hiteles elektronikus másolatainak biztonságos elektronikus tárolása is elfogadott megoldás ezen elvárás teljesítésére.

VIII. A vagyonvédelmi rendszerekhez kapcsolódó általános követelmények

29. Az MNB elvárja, hogy a pénzügyi szervezet a kockázatarányos védelmet zóna-szintű elvek alapján alakítsa ki az előzetes kockázatelemzésnek megfelelően. Elvárt továbbá, hogy a pénzügyi szervezet a védelmet legalább a nyilvános ügyfélforgalmi, továbbá a 0-24 órás üzemben működő területek, a védendő helyiségek, különösen az értékezeléssel, illetve értéktárolással összefüggő helyiségek, a bizalmas ügyfélfogadásra alkalmas helyiségek, az üzemi területek, továbbá a kapcsolódó back-office vagy támogató helyiségek, vezetői helyiségek, IT rendszerek üzemeltetéséhez szükséges, vagy az IT eszközöket koncentráltan tartalmazó helyiségek (például IT-helyiségek, számítási központok, kommunikációs központok, rendezők), tárgyalók, az átmeneti vagy tartós adat- és iratkezelés helyszínei és helyiségei, valamint az épület-üzemeltetés területeit, helyiségeit magukba foglaló épületrészek vonatkozásában biztosítsa.
30. Az MNB elvárja, hogy a pénzügyi szervezet a mechanikai-fizikai és az elektronikai védelem kialakítására kizárólag az Európai Unióban elfogadott minősítő szervezet vagy a MABISZ által kiadott, a biztonságtechnikai termék megfelelőségére vonatkozó ajánlással rendelkező, a nemzeti és az európai uniós szabványok előírásainak megfelelő eszközt alkalmazzon.
31. Az MNB elvárja, hogy a pénzügyi szervezet mérje fel, folyamatosan felügyelje, ellenőrizze és tesztelje a mechanikai-fizikai, valamint az elektronikus vagyonvédelmi rendszerek működőképességét, valamint tartsa nyilván és kísérelje figyelemmel az üzemeltetésükben, karbantartásukban részt vevő külső emberi erőforrások adatait, tevékenységét (létszám, gazdasági társaság, név, belépési jogosultság, tartózkodás és a kapcsolódó munkavégzés alapján a személy azonosításához és hitelesítéséhez szükséges adatok). Az MNB elvárja, hogy a pénzügyi szervezet a vagyonvédelmi rendszerek működőképessége tesztelésének és ellenőrzésének végrehajtását évente legalább egy alkalommal dokumentáltan is rögzítse.
32. Az MNB elvárja, hogy a pénzügyi szervezet mérje fel és kezelje a fizikai biztonsági védelmi rendszerek, valamint azok egyes elemeinek működtetéséhez kapcsolódó szerződéseket, bizonylatokat, továbbá a kapcsolattartáshoz használt elérhetőségeket.
33. Az MNB elvárja, hogy a pénzügyi szervezet azonosítsa és tartsa nyilván a mechanikai-fizikai, valamint elektronikus vagyonvédelmi rendszerek működtetésében részt vevő emberi erőforrásokat (név, feladatkör, jogosultság).
34. Az MNB elvárja, hogy a pénzügyi szervezet – lehetőség szerint a biztonsági szervezet területén belül, vagy az általa felügyelt zárt, illetéktelenek hozzáférése ellen védett, a védendő helyiségekre vonatkozó előírásoknak megfelelő területeken, ellenőrzött körülmények között – tárolja a mechanikai-fizikai, valamint elektronikus vagyonvédelmi rendszerek biztonságos működtetéséhez szükséges jogosultságokat, kódokat, kulcsokat, illetve biztosítsa az azok

biztonságos elkülönítéséhez és tárolásához szükséges erőforrásokat (például értéktároló szekrény, elektronikus adathordozó, biztonsági tároló).

35. Elvárt, hogy a pénzügyi szervezet önállóan, biztonsági szervezete útján, vagy amennyiben a feladatot külső szolgáltató látja el, a szolgáltatóval együttműködve felmérje a működtetett vagyonvédelmi rendszer és rendszerelemek elhelyezkedését és azt tervrajzra, annak hiányában helyszínrajzra felvezesse, amelynek bizalmasságát és integritását megfelelő intézkedésekkel megóvjá.
36. Az MNB elvárja azt is, hogy a pénzügyi szervezet kísérje figyelemmel a mechanikai-fizikai és az elektronikus vagyonvédelmi rendszerek, rendszerelemek típusát, üzembehelyezésének idejét, az üzembehelyező, karbantartó azonosítására alkalmas, valamint az üzembehelyezővel, karbantartóval történő kapcsolattartására vonatkozó adatokat, a szolgáltatás igénybevétele során alkalmazott egyedi, azonosításra alkalmas aktiváló és lemondó jelszavakat vagy kódokat, illetve azok cseréjének tervezhetősége miatt az eszközök üzemidőhöz viszonyított avultságát és teljesítményük mértékét.

IX. Mechanikai-fizikai védelem, helyiségek védelme

37. Az MNB elvárja, hogy a pénzügyi szervezet a biztonsági szabályzatában foglaltak alapján az elhelyezésére szolgáló épület (épületrész) és a védendő helyiségekben folyó tevékenység figyelembevételével kockázatelemzést végezzen, és ez alapján gondoskodjon a védendő helyiségek mechanikai-fizikai védelméről.
38. Az MNB elvárásainak megfelelően a pénzügyi szervezet a kockázatértékelés alapján biztosítja, hogy
 - a) az elhelyezésére szolgáló épület (épületrész) külső határoló felületei megfeleljenek a MABISZ által közzétett „Betöréses lopás- és rablásbiztosítás technikai feltételei” című ajánlásban meghatározott, legalább a részleges mechanikai-fizikai védelem követelményeinek, valamint a nemzeti és az európai uniós szabványok előírásainak; valamint
 - b) az értéktároló helyiségek határoló felületeinek minősége megfeleljen a MABISZ által közzétett „Betöréses lopás- és rablásbiztosítás technikai feltételei” című ajánlásban meghatározott teljeskörű mechanikai-fizikai védelem követelményeinek. Ez alól kivételt képezhetnek a bankjegykiadó automaták – amelyekben a MABISZ vagyonvédelmi és kármegelőzési bizottsága által meghatározott kockázatvállalási értékhatárnak megfelelő összeg tárolható – és a tíz millió forintot meg nem haladó értéket tároló páncélszekrények elhelyezésére szolgáló helyiségek.
39. Az MNB elvárása szerint a pénzügyi szervezet ügyfélfogadásra olyan helyiséget biztosít, amely alkalmas az ügyfelek fogadására, kiszolgálására, lehetővé teszi a bizalmas ügykezelést és eleget tesz a jelen ajánlásban foglalt biztonsági feltételeknek.

40. Amennyiben a helyiség a pénzügyi szervezet kizárólagos használatában lévő épületben (épületrészben) üzemel, úgy az MNB elvárja, hogy a védendő helyiség védelmét a pénzügyi szervezet az épület egészének védelmi rendszerébe illessze.

X. Elektronikai védelem

41. Az MNB elvárja, hogy a pénzügyi szervezet a biztonsági szabályzatában meghatározottak és a kockázatértékelés alapján, a MABISZ által közzétett „Betöréses lopás- és rablásbiztosítás technikai feltételei” című ajánlásban meghatározott elektronikai jelzőrendszer követelményeinek, valamint a nemzeti és az európai uniós szabványok előírásainak megfelelő védelmi rendszerrel gondoskodjon a védendő helyiségek elektronikai védelemmel való ellátásáról.

42. Az MNB elvárja, hogy az elektronikus vagyonvédelmi rendszereket lehetőség szerint

- a) a biztonsági szervezet vezetője, a biztonságért felelős személy által jóváhagyott terv alapján telepítse a pénzügyi szervezet,
- b) a külön jogszabályban előírt szakvizsgával, szakképesítéssel rendelkező személy, illetve hatósági engedéllyel rendelkező szervezet tervezze, telepítse és tartsa karban, amely személy vagy szervezet egyben titoktartási kötelezettséget is vállal a védelmi rendszer működésére vonatkozóan, és megfelelő működésüket időszakosan ellenőrizze.

43. Az MNB szükségesnek tartja, hogy az elektronikus vagyonvédelmi rendszerek programozásához és a kezelői jogosultság kiadásához szükséges kódok a biztonsági szervezet vezetőjénél, a biztonságért felelős személynél vagy az általuk írásban felhatalmazott személynél rendelkezésre álljanak.

44. Az MNB elvárja, hogy a pénzügyi szervezet gondoskodjon a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény 74. § 7. pontjában meghatározott távfelügyeleti rendszer kiépítéséről és működtetéséről.

XI. Pénz- és értéktárolás, kezelés védelme

45. Az MNB elvárja, hogy a pénzügyi szervezet a jogszabályi előírásokkal összhangban pénzkezelési szabályzatot készítsen. Ezen túlmenően az MNB elvárja, hogy a pénzügyi szervezet értékkezelési szabályzattal rendelkezzen. Az értékkezelési szabályzat az MNB elvárása szerint tartalmazza az értéktárban dolgozók feladatait és hatásköreit, az összeférhetlenségi szabályokat, a nyitás és zárás különleges eljárásait, a kulcsok használatát, a nyilvántartási rendet és az ellenőrzési feladatokat.

46. Elvárt, hogy a pénzügyi szervezet a pénz és értékpapír nem ügyfelektől történő fizikai átvételét és kiadását – az ügyfélforgalmi időn kívüli időszakot kivéve – lehetőség szerint az ügyféltértől

elkülönített helyiségben; ügyfelektől az értéktártól elkülönített, elektronikus vagyónvédelmi eszközökkel ellátott helyiségben végezze.

47. Elvárt, hogy az ügyfél kérésére a pénz és értékpapír átvételét és kiadását a pénzügyi szervezet az ügyféltértől elkülönített helyiségben biztosítsa.
48. A kizárólag pénztárként üzemelő kiszolgáló pontok a kockázatértékelés alapján minden oldalról zártak és benyúlás ellen védettek az MNB elvárása szerint. Az MNB javasolja, hogy az alkalmazott időzárás eszközökön kívül tartott érték – felügyelet biztosítása mellett – a kétfélmillió forintot ne haladja meg, valamint azt, hogy a pénztárhelyiségben csak a pénztárossal együtt tartózkodjon más, jogosultsággal rendelkező személy.
49. Az MNB elvárja, hogy az egyponstos ügyfélkiszolgálásra kialakított munkahelyek esetében a pénzügyi szervezet a nyitott pultrendszer mellett olyan automatikus pénzkidó berendezést, illetve időzárás kasszát alkalmazzon, amely az intézmény számítógépes rendszerével lehetőség szerint közvetlen kapcsolatban áll. A számítógépes rendszerrel való közvetlen kapcsolat hiánya esetén az időzárás kassza egy vagy két fiókja késleltetés nélkül lehet nyitható, azonban elvárt, hogy az ott tárolt összérték ne haladja meg a kétfélmillió forintot.
50. Elvárt, hogy a pénzügyi szervezet a 48. és 49. pontokban említett pénztárakba, valamint az egyéb, ügyfelektől pénz és értékpapír átvételére vagy kiadására használt munkahelyek esetében a MABISZ által minősített időzárás eszközöket telepítsen. Elvárt, hogy az időzárás védelem alá vont rekeszek késleltetési ideje a kockázatértékelés alapján kerüljön meghatározásra.
51. Az MNB elvárja, hogy a pénzügyi szervezet a pénztárakat és az egyéb, ügyfelektől pénz és értékpapír átvételére vagy kiadására használt munkahelyeket elektronikus támadásjelzővel is szerelje fel, és kapcsolja össze az épület vagyónvédelmi jelzőrendszerével.

XII. Letéti szolgáltatás, értékforgalom

52. Az MNB elvárja, hogy a pénzügyi szervezet letéti szolgáltatás nyújtása esetén a biztonsági kockázattal arányos védelemmel ellátott, az ügyféltértől elkülönített helyiségbe telepített betörés- és tűzbiztos³, beépített vagy rögzített, elektronikus jelzőrendszerbe bekötött páncélszekrényt vagy trezort működtessen.
53. Az MNB elvárja, hogy a pénzügyi szervezet készpénzforgalom lebonyolítása esetén a pénz és a nyomdai úton előállított értékpapír valódiságának ellenőrzésére és számolására alkalmas eszközökkel felszerelt pénztári fizetőhelyet és értéktárat, értékpapír-forgalom lebonyolítása esetén értéktárat működtessen. Kivételt képezhet a pénztári fizetőhely működtetése alól az a

³ Tűzbiztoság szempontjából elfogadható, ha az adott páncélszekrény vagy trezor a vonatkozó szabványoknak megfelel.

pénzfeldolgozási tevékenységet végző pénzügyi vállalkozás, amely más szolgáltatásával kapcsolatban készpénzforgalmat nem bonyolít le.

54. Az MNB elvárása szerint váltóval, illetve csekkel folytatott kereskedelmi tevékenység és betétgyűjtés esetében az értékpapírokat és az okmányokat a pénzügyi szervezet a szigorú számadású nyomtatványokra, illetőleg a bankjegyekre vonatkozó belső szabályzata szerint kezeli és őrzi.

XIII. Értéktárolás, értékszállítás

55. Az MNB elvárja, hogy nyitvatartási időn túl a pénzügyi szervezet
- a) az ötmillió forintot meg nem haladó összértéket beépített vagy rögzített pánccsaszekrényben tárolja,
 - b) az ötmillió forint feletti összértéket fűrés- és nyitásérzékelővel is ellátott, elektronikus jelzőrendszerbe bekötött, tanúsítvánnyal ellátott és kockázatértékelés alapján értéktároló helyiségben elhelyezett beépített vagy rögzített pánccsaszekrényben vagy trezorban tárolja,
 - c) széfet – pénzügyi szolgáltatásként – csak trezorhelyiségben vagy széf-depozitokkal bélelt, megfelelő minőségű pánccsaszekrény alkalmazásával, az erre a célra elkülönített helyiségben működtessen.
56. A pénzügyi szervezet az MNB ajánlása szerint a pénz, az értékpapír és az egyéb érték szállítását
- a) ötven millió forint összeghatárig saját szabályzatában megállapított módon,
 - b) ötven millió forint összérték felett pénzszállító szervezet igénybevételel végzi.
57. A pénzügyi szervezet különösen az alábbiakat rögzíti az 56. pont a) alpont szerinti, kizárólag a feladat ellátásával érintett személyek számára megismerhető belső szabályzatában:
- a) az előkészítő eljárás során megvalósuló kommunikáció módszere;
 - b) a tárolóeszközök meghatározása;
 - c) a tárolás módja;
 - d) a dokumentáció tartalmi és formai követelményei;
 - e) a be- és kiléptetés gyakorlata;
 - f) az értékátadás gyakorlata;
 - g) az ellenőrzés metodikája;
 - h) a különbözet esetén végrehajtandó intézkedések;
 - i) a sérülés esetén végrehajtandó intézkedések;
 - j) a szállítást végző személyzet felszerelése, kötelezettségei;
 - k) minden olyan részfeladat, körülmény, amely a tevékenység ellátásával összefügg.
58. Az értékhatár megállapításánál az értékpapír és egyéb érték esetében a piaci vagy forgalmi érték az irányadó.

XIV. Adatok, információk és adathordozók fizikai védelme

59. Az MNB elvárja, hogy a pénzügyi szervezet a biztonsági osztályba sorolás rendszerén alapuló kockázatértékelés szerint, a jelen ajánlásban foglaltakkal összhangban határozza meg az adatoknak, az iratoknak és adathordozóknak a körét, az azokhoz kapcsolódó biztonsági, hozzáférési, továbbítási, tárolási, archiválási, törlési, megsemmisítési, fizikai hozzáférés-védelmi, címkézési, kódolási és szállítási feltételeket, szabályokat és eljárásokat, valamint gondoskodjon a meghatározott védelmi intézkedések lehetőség szerint technikai kontrollokkal történő biztosításáról.
60. A jogszabályok által, illetve egyéb, a pénzügyi szervezet belső eljárásrendje szerint kötelezően védendő, üzleti működéséhez szükséges, belső szabályzatban azonosított adatok, információk, illetve az azokat tároló adathordozók fizikai és elektronikus védelme érdekében a pénzügyi szervezet meghatározza az adatokat kezelő üzleti folyamatok kiszolgálásában részt vevő elemeket – figyelembe véve a hardver és szoftver elemeken túl a távközlési és adatkommunikációs rendszereket –, valamint az adatfeldolgozásban részt vevő szervezeteket és azok infrastruktúráját, valamint osztályozza és nyilvántartja az ilyen adatokat és rendszereket tároló helyiségeket. Az MNB elvárja, hogy a pénzügyi szervezet ezeket a helyiségeket legalább folyamatos működőképességükben biztosított elektronikus vagyongvédelmi rendszerrel, valamint beépített tűzjelző berendezéssel és önműködő indítású beépített tűzoltó berendezéssel védje. A helyiségek védelmi rendszerének kiesése esetén vagy azoknak elektronikus vagyongvédelmi rendszert mellőző felügyeletére élőerős őrzés-védelem alkalmazható.
61. Elvárt, hogy az adatvagyon vonatkozásában a pénzügyi szervezet regisztráljon minden, a fizikai biztonságot érintő eseményt és minden, a működésre veszélyt jelentő incidenst, valamint a kockázatelemzésében meghatározott időközönként értékelje ki azokat. A regisztrációs állományokat (naplókat) védje az illetéktelen módosítás ellen.
62. Az MNB indokoltnak tartja, hogy az élőerős szolgáltatással összefüggő, így különösen a 27. pontban meghatározott adatok, a vagyongvédelmi rendszerrel összefüggő adatok, valamint az emberi erőforrásokra vonatkozó adatok tárolására a tűzzel szembeni ellenállóképességét legalább 30 percig megőrző, behatolásjelző rendszerbe kötött biztonsági tárolószekrényben vagy ezzel a biztonsági megoldással azonos védelmi szintet biztosító egyéb műszaki megoldással bíró helyiségben, ezek hiányában állandó élőerős őrszolgálat által védett területen kerüljön sor. A biztonsági tárolószekrény nyitásához ellenőrizhető és visszakövethető egyedi jogosultságok (például kulcs és kód) használata szükséges, amelyek kiosztását (név, jogosultság, tároló) a biztonsági szervezetenél vezetett nyilvántartásban rögzíteni, frissíteni és létezését időszakosan, de legalább évente egy alkalommal ellenőrizni szükséges.
63. Az MNB javasolja, hogy az élőerős szolgáltatással összefüggő, így különösen a 27. pontban meghatározott adatok tárolására a vagyongvédelmi rendszer dokumentációitól elkülönített módon és lehetőség szerint attól eltérő személy által kezelve kerüljön sor.

64. Az MNB indokoltnak tartja, hogy a pénzügyi szervezet a vagyonvédelmi rendszer tervezése, kivitelezése, üzemeltetése és ellenőrzése során keletkezett fizikai, illetve elektronikus adathordozókat, dokumentumokat elkülönítetten, vagyonvédelmi rendszerrel felügyelt vagy előerős őrszolgálat által védett épületrészben vagy helyiségben, a tűzzel szembeni ellenálló képességét legalább 30 percig megőrző biztonsági tárolószekrényben, vagy ezzel a biztonsági megoldással azonos védelmi szintet biztosító egyéb műszaki megoldással bíró helyiségben kezelje. A fenti adathordozók, dokumentumok biztonsági szervezet helyiségein kívüli tárolására behatolásjelzőrendszerbe kötött, a tűzzel szembeni ellenállóképességét legalább 30 percig megőrző biztonsági tárolószekrényben kerülhet sor.
65. Az MNB elvárja, hogy a pénzügyi szervezet a működését biztosító, a napi teendők ellátásához ideiglenesen nem szükséges iratokat, adathordozókat (számítógépes programok biztonsági másolatai, archivált adatok, biztonsági mentések) és a tartalékberendezéseket megfelelő védelmet biztosító elkülönített helyiségben vagy megfelelő védelmet biztosító tárolóban tárolja.
66. Az MNB elvárja, hogy a pénzügyi szervezet az archivált adatok és a biztonsági mentések egy példányát biztonságos körülmények között, fizikailag elkülönített helyen, tűzbiztos módon tárolja.

XV. Az emberi erőforrás biztonságát érintő és az emberi erőforrás irányából felmerülő kockázatok

67. Az MNB elvárja, hogy a pénzügyi szervezet önállóan, biztonsági szervezete útján vagy amennyiben a feladat külső szolgáltató igénybevétele útján kerül ellátásra, a külső szolgáltatóval együttműködve a kockázatelemzés során mérje fel a működésében részt vevő belső emberi erőforrásaiból származó vagy személyüket érő kockázatokat, tervezze meg a kockázatkezeléssel összefüggő, kockázatkerülésre felkészítő képzési stratégiáját, illetve alkossa meg az azonosított humánkockázatok kezelésével összefüggő eljárásait. Elvárt továbbá, hogy a pénzügyi szervezet az emberi erőforrás biztonságát a kockázatelemzés eredményeire alapuló, arányos intézkedéseivel biztosítsa.
68. Ehhez kapcsolódóan az MNB jó gyakorlatnak tartja, ha a pénzügyi szervezet
- a) az emberi erőforrások biztonságát érintő vagy irányából felmerülő kockázatok becsléséhez, kezeléséhez meghatározza, illetve munkaköre alapján besorolja a veszélyeztetett emberi erőforrásokat;
 - b) az előzetes kockázatelemzés és a biztonsági tervezés során figyelembe veszi a feladatkör jellegét (például érték- vagy ügyfélkezelési funkció, egyes back-office feladatok);
 - c) a kockázatelemzés eredményeire alapulóan, illetve saját értékelése szerint időszakos, az emberi erőforrás feladatai ellátásának megbízhatóságára irányuló ellenőrzéseket végez;
 - d) segíti és támogatja a visszaéléses típusú (belső, külső csalás, visszaélés, illetve egyéb, a vagyoni értékeket, üzleti célokat és jó hírnevet sértő vagy veszélyeztető) belső és külső

emberi erőforrással megvalósított cselekmények megelőzését, felderítését, vizsgálatát; valamint

- e) megelőző, biztonságtudatosító, felkészítő tevékenységet, oktatást végez a munkavállalói és vezetői körben egyaránt.

XVI. Incidenskezelés

69. Elvárt, hogy biztonsági incidens, illetve a humánkockázati incidens bekövetkezése esetén az elsődleges azonosító vagy kárenyhítő intézkedéseket a pénzügyi szervezet a biztonsági szervezet eljárásrendje alapján önállóan hajtsa végre, a további tényfeltáró intézkedéseket önállóan vagy az arra jogosult saját kontrollszerkezettel, személyllyel közösen, illetve amennyiben jogszabályi kötelezettsége fennáll, a külső hatósággal együttműködve hajtsa végre és összegezze.
70. Elvárt, hogy a pénzügyi szervezet a biztonsági incidenseket, illetve humánkockázati incidenseket követően gondoskodjon az érintett munkavállalói vagy a külső szolgáltató ismételt és frissített biztonsági felkészítéséről, valamint a pénzügyi szervezet vezetőjének tájékoztatásáról az incidenskezelés során tett megállapításokról.

XVII. Egyéb ajánlások

71. Az MNB ajánlja, hogy a pénzügyi szervezet a nála elhelyezett értékekre vagyonszozosítást kössön, amely a széfszolgáltatás kivételével teljeskörű. A vagyonszozosítási szerződésben, illetve annak mellékletében megtörténik a biztosított vagyonelemek felsorolása, értéke (amennyiben ezeket az adatokat a pénzügyi szervezet nem ismeri, pl. a széfszolgáltatás esetében, akkor a biztosítási értékhatár) és azok fizikai elhelyezésének meghatározása, helyváltoztatás esetén a lista (biztosító felé is jelzett) aktualizálása.
72. Amennyiben a pénzügyi szervezet, illetve az általa használt rendszer a pénzügyi ágazathoz tartozó európai vagy nemzeti létfontosságú rendszerelemként került kijelölésre, akkor a pénzügyi szervezet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendeletben meghatározott eljárásnak megfelelően felméri és naprakészen kezeli a jogszabályok alapján azonosított és besorolt létfontosságú rendszerelemmé kijelölt infrastruktúráját és annak védelmi környezetét.

XVIII. Záró rendelkezések

73. Az ajánlás a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 13. § (2) bekezdés i) pontja szerint kiadott, a felügyelt pénzügyi szervezetekre kötelező erővel nem rendelkező szabályozó eszköz. Az MNB által kiadott ajánlás tartalma kifejezi a jogszabályok által támasztott

követelményeket, az MNB jogalkalmazási gyakorlata alapján alkalmazni javasolt elveket, illetve módszereket, a piaci szabványokat és szokványokat.

74. Az ajánlásnak való megfelelést az MNB az általa felügyelt pénzügyi szervezetek körében az ellenőrzési és monitoring tevékenysége során figyelemmel kíséri és értékeli, összhangban az általános európai felügyeleti gyakorlattal.
75. Az MNB felhívja a figyelmet arra, hogy a pénzügyi szervezet az ajánlás tartalmát szabályzatai részévé teheti. Ebben az esetben a pénzügyi szervezet jogosult feltüntetni, hogy vonatkozó szabályzatában foglaltak megfelelnek az MNB által kiadott vonatkozó számú ajánlásnak. Amennyiben a pénzügyi szervezet csupán az ajánlás egyes részeit kívánja szabályzataiban megjeleníteni, úgy az ajánlásra való hivatkozást kerülje, illetve csak az ajánlásból átemelt részek tekintetében alkalmazza.
76. Az MNB a jelen ajánlás alkalmazását 2021. április 1-jétől várja el az érintett pénzügyi szervezetektől figyelemmel a 77. pontban foglaltakra.
77. Az MNB elvárja, hogy amennyiben a pénzügyi szervezet a jelen ajánlásban foglaltaknak annak közzétételkor nem felel meg, dolgozzon ki intézkedési tervet arra vonatkozóan, hogy milyen ütemezésben kívánja biztonsági előírásait és gyakorlatát fejleszteni. Elvárt, hogy a pénzügyi szervezet a kidolgozott intézkedési tervet 2021. március 31-ig küldje meg az MNB részére.
78. 2021. április 1-jén hatályát veszti a Pénzügyi Szervezetek Állami Felügyelete elnökének a pénzügyi szervezetek működésének biztonsági feltételeiről szóló 10/2001. számú ajánlása

Dr. Matolcsy György sk.
a Magyar Nemzeti Bank elnöke

A működés biztonsági feltételeinek kialakítását meghatározó és befolyásoló szabályozó eszközök a jelen ajánlás kiadásának időpontjában

I. Törvények

1993. évi XCVI. törvény az önkéntes kölcsönös biztosító pénztárakról

1994. évi XLII. törvény a Magyar Export-Import Bank Részvénytársaságról és a Magyar Exporthitel Biztosító Részvénytársaságról

1996. évi CXIII. törvény a lakástakarékpénztárakról

1997. évi XXX. törvény a jelzálog-hitelintézetéről és a jelzáloglevélről

1997. évi LXXXII. törvény a magánnyugdíjról és a magánnyugdíj pénztárakról

1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és mezei őrszolgálatról

2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról

2001. évi CXX. törvény a tőkepiacról

2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól

2009. évi CLV. törvény a minősített adat védelméről

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

2012. évi C. törvény a Büntető Törvénykönyvről

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013. évi V. törvény a Polgári Törvénykönyvről (Második könyv, Harmadik rész, Személyiségi jogok)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2013. évi CCXXXV. törvény az egyes fizetési szolgáltatókról

2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról

2013. évi CXXXIX. törvény a Magyar Nemzeti Bankról

2014. évi LXXXVIII. törvény a biztosítási tevékenységről

2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

2018. évi LIV. törvény az üzleti titok védelméről

II. Rendeletek

98/1995. (VIII. 24.) Kormányrendelet az egyes értékpapírok előállításának, kezelésének és fizikai megsemmisítésének biztonsági szabályairól

253/2004. (VIII. 31.) Kormányrendelet a fegyverekről és lőszeréről

22/2008. (II. 7.) Kormányrendelet a befektetési szolgáltatási tevékenységet, befektetési szolgáltatási tevékenységet kiegészítő szolgáltatást, valamint árutőzsdei szolgáltatást folytató gazdálkodó szervezet üzletszabályzatának kötelező tartalmi elemeiről

35/2009. (XII. 28.) MNB rendelet a fizetési rendszer működtetésére vonatkozó tárgyi, technikai, biztonsági és üzletmenet-folytonossági követelményekről

90/2010. (III. 26.) Kormányrendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

65/2013. (III. 8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

41/2015. (VII. 15.) BM rendelet 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

42/2015. (III. 12.) Kormányrendelet a pénzügyi intézmények, a biztosítók és viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

330/2015. (XI.10.) Kormányrendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2016/679 (EU) európai parlamenti és tanácsi rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

III. Ajánlások

A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről

A Magyar Nemzeti Bank 7/2020. (VI. 3.) számú ajánlása a külső szolgáltatók igénybeviteléről

A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybeviteléről

A Magyar Nemzeti Bank 26/2018. (VIII.16.) számú ajánlása a pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekről

A Magyar Nemzeti Bank 27/2018. (XII.10.) számú ajánlása a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról

A Magyar Nemzeti Bank 15/2015. számú ajánlása az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról

A MABISZ ajánlása a betöréssel lopás- és rablásbiztosítás technikai feltételeiről

IV. Szabványok

Biztonságtechnikai, vagyonvédelmi és tűzvédelmi szabványok