

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

I. AZ AJÁNLÁS CÉLJA ÉS HATÁLYA

A pénzügyi közvetítőrendszer tagjainak kiemelten gondoskodniuk kell az informatikai rendszerük védelméről, a saját és a gondjaikra bízott ügyfélvagyon, valamint az ügyfelek adatai – minden, az ügyfél azonosítására vagy szokásaira, különleges helyzetére közvetlenül alkalmas vagy közvetve utaló adata (a továbbiakban: ügyféladat) – illetve adó-, üzleti, bank-, értékpapír-, pénztár-, fizetési, biztosítási vagy foglalkoztatói nyugdíjtítka (a továbbiakban együtt: pénzügyi ágazati titok) védelme érdekében. Az egyes pénzügyi tevékenységekre vonatkozó ágazati törvények¹ rendelkezései mellett a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről külön kormányrendelet (a továbbiakban: Kormányrendelet) is rendelkezik².

Az ajánlás célja, hogy a pénzügyi közvetítőrendszer tagjai számára gyakorlati útmutatást adjon informatikai rendszerük védelmének kockázatokkal arányos kialakításban, valamint azok védelmére vonatkozó jogszabályi rendelkezések alkalmazásának egységes értelmezésében. Az ajánlás az egyes témaköröket, keretszabályokat meghatározó jogszabályi rendelkezésekből elsősorban a Kormányrendelet szabályait ismerteti, az ágazati törvények szövegezése ettől kis mértékben eltérhet. Az ajánlás a jogszabályi rendelkezésekben meghatározott védelmi területeken felmerülő kockázatok alapján határozza meg az elvárt intézkedéseket, és javasol az elvárások teljesítésével kapcsolatos legjobb gyakorlatot (a továbbiakban: előremutató gyakorlat). Az előremutató gyakorlatok mindegyikének egyidejű kialakítása nem minden esetben célszerű, mivel sokszor egymás kompenzáló kontrolljaként is értelmezhetők. Az elvárások más megoldásokkal is teljesíthetők, feltéve, hogy az adott elvárás kockázatcsökkentő célja teljesül.

Az ajánlás a felügyeleti vizsgálati tapasztalatok és az általános informatikai biztonság kibocsátáskor ismert és elvárható követelményei alapján készült.

A jogszabályi rendelkezések lehetővé teszik, hogy a pénzügyi közvetítőrendszer tagjai az informatikai tevékenységet csak részben lássák el saját maguk, annak egy részét vagy egészét kiszervezhetik azzal, hogy a kiszervezett tevékenységért való végső felelősség a megbízót terheli. Az ajánlás – e jogszabályi rendelkezéssel összhangban – a kiszervezés informatikai biztonsági vonatkozásaira is kitér.

¹ a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (a továbbiakban: Hpt.) 67. § (1) bekezdés d) pontja és 67/A. §-a,

az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 12. § (1) bekezdés d) pontja és (3) bekezdése, valamint 12/A. §-a, a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységekről szóló 2007. évi CXXXVIII. törvény (a továbbiakban: Bszt.) 12. §-a,

a tőkepiacról szóló 2001. évi CXX. törvény 318/D. §-a alapján a Bszt. 12. §-a,

a kollektív befektetési formákról és kezelőikről, valamint egyes pénzügyi tárgyú törvények módosításáról szóló 2014. évi XVI. törvény 29. és 30. §-a,

a magánnyugdíjról és a magánnyugdíj-pénztárakról szóló 1997. évi LXXXII. törvény (a továbbiakban: Mpt.) 77/A. §-a,

az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény (a továbbiakban: Öpt.) 40/C. §-a,

a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 94. § (1) bekezdés c) pontja és (3)-(6) bekezdése,

² a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet

Jelen ajánlás címzettjei a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény (a továbbiakban: MNB tv.) 39. §-ában meghatározott jogszabályok hatálya alá tartozó szervezetek és személyek (a továbbiakban együtt: intézmény).

Jelen ajánlás a közösségi és publikus felhőszolgáltatás igénybevételéről szóló 4/2019. (IV. 1.) MNB ajánlásban³ foglaltakkal, valamint az elektronikus úton megkötött írásbeli szerződésekről, megtett írásbeli jognyilatkozatokról szóló Vezetői körlevéllel⁴, a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról szóló 27/2018 (XII.10.) MNB ajánlással, valamint a külső szolgáltatók igénybevételéről szóló MNB ajánlással⁵ együtt alkalmazandó.

Jelen ajánlás a jogszabályi rendelkezésekre teljeskörűen nem utal vissza az elvek és elvárások megfogalmazásakor, az ajánlás címzettjei a kapcsolódó jogszabályi előírásoknak való megfelelésre azonban természetesen 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 értelmezhetőek személyes adatok kezelésére vonatkozó felhatalmazásnak. Az ajánlásban rögzített felügyeleti elvárások teljesítésével összefüggésben történő adatkezelés kizárólag a mindenkor hatályos adatvédelmi jogszabályi rendelkezések betartásával végezhető.

II. TERVEZÉS, SZERVEZET, SZABÁLYOZÁS, KOCKÁZATELEMZÉS

1. AZ INFORMATIKAI TERVEZÉS ÉS SZERVEZET

1.1. Az informatikai vállalatirányítás és tervezés dokumentumai

1.1.1. Vonatkozó jogszabályi rendelkezés: *a szabályozási rendszerben meg kell határozni az információ-technológiával szemben támasztott követelményeket, a használatából adódó biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokat az informatikai vállalatirányítás, a tervezés, a fejlesztés és a beszerzés, valamint az üzemeltetés, a monitorozás és független ellenőrzés területén.*⁶ *Az intézménynek rendelkeznie kell az informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, a fejlesztésre vonatkozó tervekkel.*⁷

1.1.2. Az informatikai költségek, beruházások, fejlesztések az üzleti célokat, igényeket szolgálják, az informatikai védelmi intézkedések az üzleti folyamatok alapján felmért kockázatok megfelelő csökkentésére hivatottak. Az informatikai beruházások öncélúan nem értelmezhetőek, azok minden esetben – közvetlenül vagy közvetve – valamilyen üzleti folyamatot, vagy annak kockázatarányos védelmét szolgálják. Ezért az intézmény az üzleti stratégiájára alapozva meghatározza az informatikai (vállalat-)irányítás és tervezés szabályzatait, az alábbiak szerint:

³ <https://www.mnb.hu/letoltes/4-2019-felho.pdf>

⁴ <https://www.mnb.hu/letoltes/ejognyil-korlevel.pdf>

⁵ Kidolgozás alatt.

⁶ Bszt. 12. § (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Kormányrendelet 2. § (1) bekezdése

⁷ Bszt. 12.§ (7) bekezdés a) pontja, Mpt. 77/A. § (6) bekezdés a) pontja, Öpt. 40/C. § (6) bekezdés a) pontja, Kormányrendelet 3. § (3) bekezdés a) pontja

1.1.3. Az informatikai (vállalat-)irányítás és tervezés szabályzatai összhangban vannak az intézmény üzleti céljaival, figyelembe véve az informatikai- és adatkommunikációs technológiai és információbiztonsági irányokat. Az intézmény az informatikai tervezés során elkészíti legalább az alábbi dokumentumokat:

- a) informatikai stratégia,
- b) éves informatikai beruházási és költség tervek.

1.1.4. Az információbiztonsági elvek megfelelő érvényesülése érdekében az IT stratégiai dokumentumok mindenkor az informatikai biztonsági funkció közreműködésével és jóváhagyásával készülnek.

1.1.5. Az intézmény az IT stratégiai dokumentumokban az elérni kívánt célokra vonatkozóan megfogalmaz legalább az IT infrastruktúrára, architektúrára, a működésre, az üzleti területet kiszolgáló legfontosabb alkalmazásokra és a kiszervezésre vonatkozó elvárt, elérendő állapotokat.

1.1.6. Az intézmény az IT stratégiában rögzített célok megvalósulását rendszeresen – a dokumentum időbeli hatályával összhangban legalább évente – dokumentáltan nyomon követi, a stratégiában foglaltaktól való eltérést kiértékeli.

1.2. Szervezeti és működési rend

1.2.1. Vonatkozó jogszabályi rendelkezés: *az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével az intézmény meghatározza a szervezeti és működési rendeket, a felelősségi, a nyilvántartási és a tájékoztatási szabályokat.*⁸

1.2.2. Az intézmény az informatikai szervezetének felépítését és működését a szervezeti és működési szabályzatában rögzíti, és az informatikai munkakörkhöz rendeli a feladatokat és felelőségeket a dolgozók által tudomásul vett, és a tudomásul vételt igazoló dokumentumokban (például munkaköri leírásokban).

1.2.3. Az intézmény az üzleti működésének jellegére, nagyságrendjére figyelemmel alakítja ki informatikai szervezetét, felelősségi köreit, annak működési rendjét, nyilvántartási- és a tájékoztatási szabályait.

1.2.4. Az intézmény úgy alakítja ki az informatikai biztonsági funkciót, illetve szervezetet, valamint úgy határozza meg a vonatkozó feladatokat, hogy az arányban álljon informatikai biztonsági kockázataival, ennek keretében gondoskodik legalább az informatikai biztonsági funkció:

- a) feladatainak és felelőségeinek egyértelmű meghatározásáról;
- b) megfelelő szintű szervezeti függetlenségéről és a vezetői testület felé történő közvetlen elszámoltathatóságáról;
- c) összeférhetetlen szerepköreinek, eseteinek, feladatainak meghatározásáról és kizárásáról, vagy megfelelő kontrollokkal történő elkülönítéséről;
- d) megfelelő szakismeretének és tevékenységének időszakos ellenőrzéséről
- e) folyamatos képzéséről.

1.2.5. Az informatikai biztonságért az intézmény legfelső operatív vezetője a felelős, aki a feladatkört delegálhatja.

2. INFORMATIKAI BIZTONSÁGI SZABÁLYOZÁSI RENDSZER

2.1. Az informatikai biztonsági szabályozási rendszer alapelvei

⁸ Bszt. 12. § (4) bekezdése, Mpt. 77/A. § (3) bekezdése, Öpt. 40/C. § (3) bekezdése, Kormányrendelet 2. § (3) bekezdése

- 2.1.1. *Vonatkozó jogszabályi rendelkezés: az intézmény kialakítja a pénzügyi szolgáltatási, a kiegészítő pénzügyi szolgáltatási, biztosítási és viszontbiztosítási és az azzal közvetlenül összefüggő tevékenységének, a befektetési szolgáltatási tevékenységének és kiegészítő szolgáltatásának ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét, valamint gondoskodik az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben meg kell határozni az információ-technológiával szemben támasztott követelményeket, a használatából adódó biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokat az informatikai vállalatirányítás, a tervezés, a fejlesztés és a beszerzés, valamint az üzemeltetés, a monitorozás és független ellenőrzés területén.*⁹
- 2.1.2. A szabályozási rendszer alatt a követendő viselkedésminták, szabályok, eljárások folyamatos meghatározását, bevezetését, betartását, betartatását (kikényszerítését), szankcionálását, ellenőrzését, felülvizsgálatát, aktualizálását (visszacsatolását), valamint az ellenőrzések során feltárt hiányosságok megszüntetését, illetve ezek eljárásrendjét, dokumentálását, formális jóváhagyását és az érintettekkel való ismertetését (közzétételét) kell érteni.
- 2.1.3. Az informatikai biztonsági szabályozási rendszer az informatikai és adatkommunikációs rendszerek védelmére, a rendszerek biztonságos működésére és működtetésre vonatkozó szabályozási rendszer. Ennek célja, hogy elvárások meghatározásán keresztül csökkentse a nem kívánt tevékenységből, az információ hiányából és az elvégzett tevékenységek dokumentálásának elmaradásából származó, informatikai jellegű működési kockázatokat. A megfelelő informatikai biztonsági szabályozási rendszer az intézmények informatikai biztonságának közvetett, megelőző kockázatcsökkentő kontrollja, amely teljeskörűsége és folyamatos megfelelése az intézménynél elvárt magatartás és teljesítés számonkérésének alapja.
- 2.1.4. Az informatikai biztonsági szabályozási rendszer kialakításakor az intézmény gondoskodik arról, hogy a szabályozási rendszere illeszkedjen pénzügyi tevékenysége jellegéhez, legyen arányos annak nagyságrendjével és összetettségével, álljon összhangban az informatikai rendszer kockázatokkal arányos védelmét biztosító eszközrendszerrel.
- 2.1.5. Az intézmény biztosítja, hogy a kockázataival arányos adminisztratív védelmi intézkedései a védendő adat-, információ és eszközvagyon feltérképezésén és osztályozásán, valamint az azokat fenyegető kockázatok felmérésén alapulnak, és a hatályos jogszabályi környezetből levezethető, az intézményre jellemző részletszabályokat tartalmaznak.
- 2.1.6. Az intézmény a szabályzatokat a szabályozási rendszerben meghatározott eljárásrend alapján, dokumentáltan hatályba lépteti és a személyi hatálya alá tartozók számára megfelelően ismerteti, a szabályok megismerését dokumentálja, a hatályban lévő szabályzatok elérhetőségét egyértelműen meghatározza.
- 2.1.7. A szabályzatokban (vagy a szabályzatok rendszeréről szóló szabályzatban) az intézmény rendelkezik a szabályzat felülvizsgálatának és aktualizálásának gyakoriságáról és felelőseiről, dokumentálásának eljárásrendjéről. A szabályzatokat felülvizsgálja és aktualizálja minden jogszabályi, szabályozási vagy alkalmazási környezetben vagy munkafolyamatban bekövetkező lényegi változás esetén, de legkésőbb a kockázatelemzés felülvizsgálatához kapcsolódóan.
- 2.1.8. A szabályozási rendszer elemeinek rendelkezései egyértelműek, világosak, könnyen érthetők, betarthatók és betartathatók.

⁹ Bszt. 12. § (1) és (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Kormányrendelet 2. § (1) bekezdése

2.1.9. A szabályozások kialakításakor az intézmény meghatározza a szabályzatok személyi, tárgyi és területi hatályát, különös tekintettel arra, hogy az egyes szabályzatok csak azok számára legyenek alkalmazandók és váljanak megismerhetővé, akiknek feltétlenül szükséges.

2.1.10. Az informatikai biztonsági szabályozási rendszer elkészítésekor az intézmény figyelembe vehet iparági szabványokat, útmutatókat, módszertanokat, de az MNB elvárja, hogy a szabályozás mindenkor az intézmény működéséhez illeszkedjen. A szabályozásban nem írhatók elő olyan gyakorlatok, amelyek az intézmény szempontjából nem relevánsak, nem életszerűek, technikailag kivitelezhetetlenek, a kockázatokkal nem állnak arányban, nincsenek összhangban az intézmény működésével vagy betarthatatlanok.

2.2. Biztonsági osztályba sorolási rendszer

2.2.1. Vonatkozó jogszabályi rendelkezés: *az intézménynél mindenkor rendelkezésre kell állnia az informatikai rendszer elemeinek az intézmény által meghatározott biztonsági osztályokba sorolási rendszerének.*¹⁰

2.2.2. Az adatgazda adatbiztonsági osztályokba sorolja az adatokat, bizalmosságukat, sértetlenségüket és rendelkezésre állásukat érintő kockázatok alapján. Az adatgazda az adatkategóriákhoz – a kockázatokkal arányosan – meghatározza legalább az adatokkal kapcsolatos biztonsági: hozzáférési, továbbítási, tárolási, archiválási, törlési, megsemmisítési, fizikai hozzáférés-védelmi, címkézési, kódolási és szállítási feltételeket, szabályokat és eljárásokat. Az adatgazda 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 – az érintett adatok besorolása szerinti védelmi osztályokba sorolja. A jelen pont szerinti rendszer együttesen a biztonsági osztályba sorolás rendszere.

2.2.3. Az intézmény a biztonsági osztályokba sorolás rendszerével kapcsolatos szabályokról és eljárásrendekről az informatikai biztonsági szabályozási rendszerében rendelkezik.

2.2.4. Az intézmény adatainak biztonsági osztályokba sorolási rendszere összhangban van a pénzügyi ágazati titokra, illetve a személyes adatok védelmére vonatkozó jogszabályi rendelkezésekkel, az intézmény adatvédelmi előírásaival.

2.2.5. Az intézmény az ügyféladatot és pénzügyi ágazati titkot (ideértve az érzékeny fizetési adatot is), az ezekből – visszafejthető módon – származtatott adatokat, valamint az ezeket feldolgozó rendszereket és infrastruktúra elemeket a legszigorúbb biztonsági osztályba sorolja.

2.2.6. A 2.2.5. pontban meghatározott legszigorúbb biztonsági osztálynál az intézmény abban az esetben határozhat meg szigorúbb biztonsági besorolást, ha az ahhoz tartozó védelmi intézkedések konkrétan nevesítik az adathoz hozzáférő természetes személyeket.

2.3. Az adatgazda és a rendszergazda kijelölését tartalmazó dokumentum

2.3.1. Vonatkozó jogszabályi rendelkezés: *az intézménynél mindenkor rendelkezésre kell állnia az adatgazda és a rendszergazda kijelölését tartalmazó dokumentumnak.*¹¹

¹⁰ Bszt. 12. § (9) bekezdés c) pontja, Mpt. 77/A. § (7) bekezdés c) pontja, Öpt. 40/C. § (7) bekezdés c) pontja, Kormányrendelet 4. § (1) bekezdés c) pontja

¹¹ Bszt. 12. § (9) bekezdés e) pontja, Mpt. 77/A. § (7) bekezdés e) pontja, Öpt. 40/C. § (7) bekezdés e) pontja, Kormányrendelet 4. § (1) bekezdés e) pontja

- 2.3.2. Az adatgazda és a rendszergazda fontos szereplői az információbiztonság kikényszerítésének. Az adatgazda az ágazati jogszabályokban foglaltak figyelembevételével meghatározza a rá bízott adatok bizalmosságának, sértetlenségének és rendelkezésre állásának kritériumait, így az adatok biztonsági osztályát, az adatokra vonatkozó hozzáférési, módosítási, törlési, tárolási és egyéb jogosultságokat, egyéb biztonsági követelményeket, és az adatok tárolásának, mentésének, archiválásának, továbbításának és törlésének szabályait. A rendszergazda technológiailag kikényszeríti az adatgazda által meghatározott védelmi intézkedéseket.
- 2.3.3. Az intézmény rendelkezik az adatgazdák és a rendszergazdák feladatairól, felelőségeiről, kijelölésük és feladataik ellátásának eljárásrendjéről, ezek dokumentálásáról.
- 2.3.4. Az intézmény az adatgazda feladatoként meghatározza legalább a rá bízott adatvagyon adatosztályozásával, valamint az adatokhoz rendelt hozzáférési, módosítási, törlési, tárolási és egyéb jogosultságok, biztonsági követelmények, illetve az adatok tárolásának, mentésének, archiválásának, továbbításának és törlésének szabályai meghatározásával kapcsolatos feladatokat.
- 2.3.5. Az intézmény kijelöli azokat a természetes személyeket, akik az adatgazdai és a rendszergazdai feladatokat ellátják, egyértelműen és számon kérhetően összerendeli őket a gondjaikra bízott konkrét információs vagyonelemekkel.
- 2.3.6. Az intézmény az adatgazdákat és rendszergazdákat jóváhagyott eljárásrend szerint, dokumentáltan értesíti kijelölésükről, feladataikról és felelőségeikről.
- 2.3.7. Az intézmény gondoskodik annak igazoltságáról, hogy az adatgazdák és rendszergazdák elfogadták kijelölésüket, feladataikat és felelőségeiket.
- 2.3.8. Az intézmény informatikai rendszerei és üzleti folyamatai fejlesztésébe vagy átalakításába bevonja az érintett adatgazdá(ka)t is.
- 2.4. Az egyes munkakörök betöltéséhez szükséges informatikai ismeret
- 2.4.1. Vonatkozó jogszabályi rendelkezés: *az intézmény a belső szabályzatában meghatározza az egyes munkakörök betöltéséhez szükséges informatikai ismereteket.*¹²
- 2.4.2. Az intézmény gondoskodik arról, hogy a munkatársak a megfelelő ismeretek birtokában képesek legyenek az üzleti folyamatok során kezelt adatok bizalmosságát, sértetlenségét és rendelkezésre állását megfelelően biztosítani.
- 2.4.3. Az intézmény meghatározza és tételesen felsorolja az egyes üzleti és informatikai munkakörök betöltéséhez szükséges konkrét informatikai – és ezen belül az informatikai biztonsági – ismereteket, és ezt belső szabályzati rendszerében rögzíti.
- 2.4.4. Az intézmény gondoskodik arról, hogy a munkaköröket olyan személyek töltsék be, akik birtokában vannak az előírt, aktuálisan szükséges ismereteknek.

¹² Bsz. 12. § (11) bekezdése, Mpt. 77/A. § (9) bekezdése, Öpt. 40/C. § (9) bekezdése, Kormányrendelet 5. §-a

3. AZ INFORMATIKAI BIZTONSÁGI KOCKÁZATELEMZÉS, AZ INFORMATIKAI RENDSZER KOCKÁZATOKKAL ARÁNYOS VÉDELME

3.1. Kockázatelemzés

3.1.1. Vonatkozó jogszabályi rendelkezés: *az intézmény gondoskodik az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben meg kell határozni az információ-technológiával szemben támasztott követelményeket, a használatából adódó biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokat az informatikai vállalatirányítás, a tervezés, a fejlesztés és a beszerzés, valamint az üzemeltetés, a monitorozás és független ellenőrzés területén.*¹³ *Az intézmény az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétfelvévente felülvizsgálja és aktualizálja.*¹⁴ *Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja.*¹⁵ *Kockázatokkal arányos védelem: az elektronikus információrendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.*¹⁶

3.1.2. A kockázatelemzés része a kockázatfelmérés (a kockázatok azonosítása és értékelése) és a kockázatok csökkentését célzó védelmi intézkedések megtervezése. A kockázatkezelés a kockázatelemzést és a megtervezett kockázatcsökkentő védelmi intézkedések megvalósítását, ellenőrzését és javítását magába foglaló folyamat.

3.1.3. Az intézmény informatikai biztonsági kockázatelemzési és -kezelési szabályzatot készít, amelyben kitér legalább az alkalmazott információ-technológia használatából adódó, az intézményre specifikus biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokra és eljárásrendekre legalább az alábbi informatikai területeken:

- a) (vállalat-) irányítás,
- b) tervezés, fejlesztés és beszerzés,
- c) üzemeltetés,
- d) monitorozás
- e) független ellenőrzés.

3.1.4. A kockázatelemzés a kockázatokkal arányos védelem megvalósításának alapja, melynek a jogszabályi rendelkezések kiemelt jelentőséget tulajdonítanak: az intézménytől elvárt védelmi intézkedések jelentős részét a kockázatelemzés alapján indokolt, a fenyegetések által okozható károk értékével arányos feltételekhez kötik. Ha az intézmény nem rendelkezik megfelelő, aktuális, az intézményre vonatkoztatott, a releváns fenyegetéseket feltáró kockázatelemzéssel, akkor kockázatkezelési folyamata nem tudja alátámasztani jogszabályi megfelelőségét. Ezért a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank (a továbbiakban: MNB) kiemelt figyelmet fordít a kockázatelemzés dokumentáltságára, intézményi relevanciájára és aktualitására.

3.1.5. A vonatkozó jogszabályok nem szabályozzák a kockázatfelmérés elvégzésének módját (módszertanát, eljárásait, lépéseit), erről az intézmény szabadon dönt. Az MNB elvárja, hogy a kockázatfelmérés elsősorban az intézmény sajátosságait vegye figyelembe, ezért az általános érvényű kockázatfelmérési

¹³Bszt. 12. § (1) és (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Kormányrendelet 2. § (1) bekezdése

¹⁴Bszt. 12. § (3) bekezdése, Mpt. 77/A. § (2) bekezdése, Öpt. 40/C. § (2) bekezdése, Kormányrendelet 2. § (2) bekezdése

¹⁵Bszt. 12. § (7) bekezdése, Mpt. 77/A. § (6) bekezdése, Öpt. 40/C. § (6) bekezdése, Kormányrendelet 3. § (3) bekezdése

¹⁶Kormányrendelet 5/A. § (3) bekezdés c) pontja

módszertanokat csak iránymutatásként célszerű használni, mert azok olyan fenyegetéseket is részletezhetnek, amelyek az adott intézményre nem relevánsak, míg specifikus fenyegetéseket elnagyolhatnak, vagy figyelmen kívül hagyhatnak. Az általános, vagy más intézmény(ek)re optimalizált kockázatfelmérés alapján tervezett védelmi intézkedések költségei és a fenyegetések által okozható károk nem feltétlenül állnak arányban, nem a releváns fenyegetettségekre adnak választ, így nem teljesítik a jogszabályi előírásokat.

3.2. Kockázatfelmérés

3.2.1. Az intézmény az informatikai biztonsági szabályozási rendszerében előírja az informatikai rendszere biztonsági kockázatainak rendszeres időközönként történő kötelező felmérését, kijelöli a kockázatok felmérésének felelősét, és meghatározza a felmérés elvégzésének és az azt követő tevékenységek elvégzésének szabályait.

3.2.2. Az intézmény elvárható gondossággal teljeskörűen azonosítja és értékeli informatikai rendszerének biztonsági kockázatait az informatikai biztonsággal érintett valamennyi területen (informatikai (vállalat-) irányítás, tervezés, fejlesztés, beszerzés, üzemeltetés, monitorozás, független ellenőrzés).

3.2.3. Az intézmény a kockázatfelmérés során azonosított releváns kockázatokat a bekövetkezési valószínűségük és hatásuk alapján osztályozza.

3.2.4. A kockázatfelmérés eredményét – beleértve az osztályozást – az intézmény az informatikai biztonsági szabályozási rendszerében meghatározottak szerint dokumentálja és jóváhagyatja.

3.2.5. Az intézmény a kockázatfelmérés során elvégzi legalább az alábbi lépéseket:

- a) a módszertan kiválasztása, értelmezése és dokumentálása;
- b) az üzleti folyamatok meghatározása, ezen belül az adatok felmérése és osztályba sorolása, a folyamatok kockázati besorolásának elvégzése az adatok és a folyamatok bizalmosságának, sértetlenségének és rendelkezésre állásának követelményei alapján;
- c) az üzletileg kritikus, fő folyamatok azonosítása és kiválasztása;
- d) a kiválasztott folyamatok informatikai működését biztosító informatikai és adatkommunikációs szerelemek, valamint a folyamatok informatikai biztonsági szempontú sérülékenységeinek – így például kézi adatbeviteli- és módosítási lehetőségek, rendszerek közötti adatátadások, távoli hozzáférések, technikai azonosítók, megosztott adatterületek, átmeneti adatállományok, szoftver sérülékenységek, architektúra méretezés – azonosítása, dokumentálása;
- e) a szerelemekhez, valamint a sérülékenységekhez kapcsolódó informatikai biztonsági kontrollok meglétére és működésük megfelelőségére vonatkozó vizsgálatok elvégzésével a biztonsági hiányosságok és elégtelenségek azonosítása és a kockázatok értékelése, dokumentálása;
- f) az általános informatikai biztonsági kontrollok (a szerelemekhez közvetlenül nem kapcsolódó biztonsági kontrollok, mint például az emberi erőforrás, a szabályozás, az infrastruktúra területek biztonsági intézkedései) vizsgálata és értékelése, amely során az intézmény figyelembe veheti a szakmai ajánlásokat, katalógusokat¹⁷ és bevált gyakorlatokat;
- g) a szabályzati előírások és a gyakorlat összhangjának a vizsgálata;

¹⁷ például COBIT5, MSZ/T ISO/IEC 27001:2014, BSI IT-Grundschutz-Kataloge

- h) az intézmény kritikus informatikai környezetére vonatkozó informatikai biztonsági helyzetkép kialakítása, és a kockázatfelmérési jelentés dokumentum elkészítése;
- i) az intézmény a kockázatfelmérési jelentésben a vizsgált folyamatokat, rendszerelemeket, a feltárt sérülékenységeket, a vizsgálat alá vont biztonsági intézkedéseket, megállapításokat és a kockázatok mértékét, valamint a vizsgálat szempontjából releváns egyéb körülményeket teljesszűrtően dokumentálja. A dokumentum így lehetővé teszi visszaellenőrzések elvégzését, rögzíti a felmérés hatókörét, így kiinduló pontja lehet a következő időszak kockázatelemzésének;
- j) a kockázatok feltárását követően a kockázatelemzést végző és a vizsgált terület egyeztet az esetleges téves megállapítások és az eltérő kockázati értékelések feltárása érdekében;
- k) a kockázatfelmérési jelentést – legalább vezetői összefoglaló szinten – az intézmény felső vezetése tárgyalja és hagyja jóvá.

3.3. A feltárt kockázatok kezelése

3.3.1. Az intézmény a kockázatfelmérés során azonosított és osztályozott kockázatok kezelésére dokumentált és elfogadott intézkedési tervvel rendelkezik. Azokat a kockázatokot, amelyeket az intézmény nem kezel, dokumentáltan felvállalja. A kockázat felvállalás elfogadható mértékét (kockázati étvág) és szabályait előre meghatározza. Az intézmény nem vállalhat fel jogszabályi rendelkezések vagy hatósági előírások megsértésével, be nem tartásával járó kockázatokot.

3.3.2. Az intézmény az intézkedési tervben konkrét, a feltárt kockázatokhoz egyértelműen hozzárendelt, azok mértékét érdemben csökkentő feladatokat határoz meg, és megállapítja ezek erőforrás igényeit.

3.3.3. Az intézmény a feladatok végrehajtását – a kockázatok mértékével és az erőforrás igényekkel összhangban – egyértelmű véghatáridők meghatározásával ütemezi, valamint kijelöli a felelősöket. A véghatáridők nem nyúlhatnak túl a következő kockázatelemzés előírt időpontjára.

3.3.4. Az intézkedési tervet az intézmény szabályozási rendszerében kijelölt vezetője vagy vezetői testülete dokumentáltan jóváhagyja. A döntés igazolja, hogy a vezetőség a kockázatelemzés eredményét megismerte, és a feltárt, de az intézkedési tervben nem szereplő kockázatokot felvállalja.

3.3.5. Az intézkedési tervben szereplő feladatok végrehajtását az intézmény a kijelölt felelős(ök) útján nyomon követi, ellenőrzi, és amennyiben a végrehajtás a feladattervtől eltér, korrekciós intézkedéseket hoz a feladat határidőre és tervezett módon történő befejezésére.

3.3.6. A felvállalt kockázatokot az intézmény dokumentálja és az informatikai biztonsági szabályozási rendszerében meghatározott időközönként, de legkésőbb a következő kockázatelemzés során felülvizsgálja.

3.4. A kockázatelemzés felülvizsgálata

3.4.1. Az üzleti folyamatokban, az informatikai rendszerben, a vonatkozó jogszabályokban vagy szabályozási rendszerben bekövetkezett változás esetén az intézmény a változással érintett területen haladéktalanul felülvizsgálja és dokumentált módon aktualizálja kockázatelemzését.

3.4.2. Az intézmény két évente vagy annál gyakrabban az informatikai biztonságot érintő valamennyi területen, teljesszűrtően, dokumentált módon aktualizálja kockázatelemzését.

III. BESZERZÉS, FEJLESZTÉS, TESZTELÉS, VÁLTOZÁSKEZELÉS

4. KÖZÖS RENDELKEZÉSEK

- 4.1.1. Vonatkozó jogszabályi rendelkezés: *a szabályozási rendszerben meg kell határozni az információ-technológiával szemben támasztott követelményeket, a használatából adódó biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokat az informatikai vállalatirányítás, a tervezés, a fejlesztés és a beszerzés, valamint az üzemeltetés, a monitorozás és független ellenőrzés területén.*¹⁸
- 4.1.2. Az intézmény a szolgáltatási vagy kiegészítő szolgáltatási tevékenysége ellátásával kapcsolatos rendszerek és szolgáltatások beszerzésével, fejlesztésével megbízhat külső vállalkozókat. A beszerzett rendszerekért, tevékenységekért és fejlesztésekért az intézmény a felelős.
- 4.1.3. Az intézmény olyan – az informatikai biztonsági szabályozási rendszerében szabályozott – informatikai (vállalat-)irányítási megoldást alakít ki, mely lehetővé teszi az egyidőben futó informatikai projektek folyamatos, dokumentált nyomon követését, és a projektek során feltárt és a projektek közti függőségekből eredő kockázatok kezelését, teljeskörűen meghatározva és kialakítva a vonatkozó szakértői feladat- és felelősségi köröket.
- 4.1.4. Az intézmény gondoskodik arról, hogy az informatikai biztonsági funkció már a beszerzések és fejlesztések tervezésétől kezdődően (by design), azok teljes életciklusába folyamatosan bevonásra kerüljön olyan jogkörök biztosításával, amelyek lehetővé teszik a specifikációk beszerzést vagy fejlesztést megelőző és időközben változó megfelelőségének ellenőrzését, konkrét biztonsági és kontroll funkciók meghatározását, kibővítését és ezek fejlesztésének ellenőrzését és véleményezését.
- 4.1.5. A kockázatok csökkentése érdekében a beszerzések és fejlesztések vonatkozásában az intézmény az alábbi tevékenységeket végzi:

4.2. Beszerzés

- 4.2.1. Vonatkozó jogszabályi rendelkezés: *a rendszerek és szolgáltatások beszerzése szabályozott, nyomon követett, és megfelel a biztonsági előírásoknak.*¹⁹
- 4.2.2. Az intézmény az informatikai szabályozási rendszerében rendelkezik a beszerzés szabályairól és eljárásrendjéről.
- 4.2.3. Az intézmény az informatikai szabályozási rendszerében rendelkezik arról, hogy a rendszerek és szolgáltatások beszerzése esetén a szerződésbe – szerződés típusonként – milyen kötelező szerződési elemeket foglaljon.
- 4.2.4. A szolgáltatási szerződések (a továbbiakban: SLA) esetén az intézmény szerződéses feltételekkel biztosítja, hogy a szolgáltatás az intézmény részéről mérhető, számonkérhető és szankcionálható legyen (SLA követelmények érvényesítése).
- 4.2.5. Az intézmény szerződéses feltételekkel biztosítja, hogy a szerződés megszűnése esetén a szolgáltató átadja az általa közvetlenül vagy közvetve kezelt, vagy feldolgozott adatokat, a szolgáltatótól független technológia segítségével is feldolgozható formátumban.
- 4.2.6. Előremutató gyakorlat

¹⁸ Bszt. 12. § (1) és (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Kormányrendelet 2. § (1) bekezdése

¹⁹ Kormányrendelet 5/B. § 1) pontja

Az intézmény a szerződésekben rendelkezhet úgy, hogy a szolgáltatási szint mérését az intézmény maga végzi el vagy független külső szakértővel végezteti, mivel a szolgáltató által mért, utólag elszámolt SLA teljesítések az intézmény által kontrollálhatatlanok, így a nem szerződésszerű teljesítés az igazolhatóság hiányában közvetlen és közvetett károkat okozhat az intézmény számára.

4.3. Fejlesztés

4.3.1. Vonatkozó jogszabályi rendelkezés: *az intézmény rendelkezik minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működését – még a szállító, valamint a rendszerfejlesztő tevékenységének megszűnése után is – biztosítja.*²⁰ *Az intézménynél mindenkor rendelkezésre kell állnia az általa fejlesztett, megrendelésre készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek, valamint az általa fejlesztett, megrendelésre készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének.*²¹

4.3.2. Saját fejlesztésű vagy külső fejlesztő bevonásával megvalósult fejlesztések esetén az intézmény a szabályozási rendszerében rögzíti és biztosítja, hogy az üzembe helyezett rendszerek fejlesztői dokumentációja:

- a) áttekinthető formában elkészül;
- b) tartalmazza a rendszer felépítésének és működtetésének ellenőrzéséhez szükséges rendszerleírásokat és modelleket, az adatátadások szabályait, az interfész kapcsolatok leírását, a felhasználói és adminisztrátori kézikönyveket, valamint az adatok szintaktikai szabályait és tárolási szerkezetét (például üzleti- és funkcionális specifikáció, use-case-ek, rendszerterv, adatmodell, objektum-modell, adatbázis specifikáció; a jogszabályban előírt, a működtetés ellenőrzéséhez szükséges rendszerleírás vagy modell gyanánt nem fogadható el szoftverrel generált olyan dokumentáció, amelyben nem szerepel érdemi és releváns információ a dokumentált adatszerkezet, objektum, funkció, modul, program, egyéb rendszerkomponens szerepéről és működéséről);
- c) verzióként archiválásra kerül, a mindenkor aktuális és dokumentált forráskóddal együtt, egyértelműen azonosítható és az intézmény által hozzáférhető módon.

4.3.3. Amennyiben az intézmény nem végez szoftverfejlesztést, a megrendelésre készített vagy testre szabott szoftvertermékek vonatkozásában gondoskodik arról, hogy

- a) a szoftverfejlesztő a szoftver átadásával egyidejűleg átadja az adatok szintaktikai szabályait és az adatok tárolási szerkezetét is tartalmazó részletes adatbázis specifikációt, valamint a szoftver kimeneti és bemeneti adatait és a komponensek közötti adatátadások specifikációját;
- b) abban az esetben, ha a szállító a hibajavítási- vagy az alkalmazás továbbfejlesztésére vonatkozó igényeket bármilyen okból nem teljesíti, hozzájuthasson – például ügyvédi letét útján – a szoftver (dokumentált, teljeskörűen fordítható vagy fordítás nélkül futtatható állapotú, egyértelműen azonosított és aktuális) forráskód állományához és fejlesztési

²⁰ Bsz. 12. § (7) bekezdés b) pontja, Mpt. 77/A. § (6) bekezdés b) pontja, Öpt. 40/C. § (6) bekezdés b) pontja, Kormányrendelet 3. § (3) bekezdés b) pontja

²¹ Bsz. 12. § (9) bekezdés a) és b) pontja, Mpt. 77/A. § (7) bekezdés a) és b) pontja, Öpt. 40/C. § (7) bekezdés a) és b) pontja, Kormányrendelet 4. § (1) bekezdés a) és b) pontja a) b)

dokumentációjához, a forráskód alapján a futtatható kód egyértelmű előállításához szükséges folyamatok specifikációjához, és azok felett a továbbiakban jogszerűen rendelkezessen.

4.3.4. Az intézmény gondoskodik arról, hogy az alkalmazási rendszerek forráskódjaihoz, illetve informatikai rendszerleírásaihoz kapcsolódóan a kiszervezett rendszerének adatai – a visszaállási pontok és idők figyelembevételével, további felhasználásra alkalmas formátumban – mindenkor a rendelkezésére álljanak.

4.4. Tesztelés, változtatáskezelés

4.4.1. Vonatkozó jogszabályi rendelkezés: *az intézmény rendelkezik olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és a tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását.*²² *Az élesüzemi rendszer változáskezelési folyamatai biztosítják, hogy a rendszer paraméterezésében és a szoftverkódban bekövetkező változások csak tesztelt és dokumentált módon valósulhatnak meg.*²³

4.4.2. Az MNB elvárja, hogy az intézmény adatkezelőként mindenkor biztosítsa az adatok célhoz kötött kezelését. A fejlesztési és tesztelési célok nem azonosak azzal a céllal, amellyel az ügyféladat, illetve a pénzügyi ágazati titok körébe tartozó adatok felvételre kerültek, ezért elvárás, hogy a kezelt adatok sértetlensége, bizalmassága és rendelkezésre állása is biztosított legyen. Ez azt jelenti, hogy az eltérő célú adatkezelés során nem elégséges a környezetek sértetlenségi és a rendelkezésre állási szempontú szeparációjáról gondoskodni, az adatokat szükséges megfosztani azoktól a jellemzőktől, amelyek okán bizalmasnak minősülnek. Így különösen elvárás az ügyféladat és a pénzügyi ágazati titok körébe tartozó adatok felismerhetetlenné tétele minden olyan környezetben, amely az éles környezettől elkülönített (így tesztelési vagy fejlesztési) céllal működik.

4.4.3. Az intézmény az informatikai biztonsági szabályozási rendszerében rendelkezik a fejlesztések üzembe állítási és változtatáskezelési eljárásrendjéről, a dokumentálási és jóváhagyási szabályokról, a visszaállítás eljárásairól.

4.4.4. Az intézmény a fejlesztést és a tesztelést az élesüzemi környezettől elkülönített környezetekben végzi.

4.4.5. Az intézmény nem, vagy csak teljeskörű anonimizálást követően használ éles rendszerből vett adatokat a fejlesztői és a teszt környezetben. A közvetlen élesítést megelőző tesztelési illetve hibakeresési eljárás során éles adat csak akkor kezelhető a teszt környezetben, ha a tesztkörnyezetre vonatkozó kontrollok megegyeznek vagy szigorúbbak az éles rendszerekre vonatkozó kontrolloknál és az élesítési vagy hibakeresési teszt környezet egyedileg, teljes körűen dokumentált eljárásban, a vezetés által jóváhagyott módon, meghatározott időintervallumra és felhasználói körre kerül kialakításra, valamint a tesztelési eljárást követően a teszt környezetből az éles adatok azonnal törlésre kerülnek.

4.4.6. A futtatható kód éles üzembe állítását a fejlesztőtől független funkció végzi, aki egyben gondoskodik a forrás- és a futtatható kód azonosításáról és tárolásáról, a verziók közötti különbségek dokumentálásáról, valamint a tesztelt, az élesítésre jóváhagyott és az élesüzembe állított verziók azonosságának ellenőrzéséről.

²² Bsz. 12. § (7) bekezdés d) pontja, Mpt. 77/A. § (6) bekezdés d) pontja, Öpt. 40/C. § (6) bekezdés d) pontja, Kormányrendelet.3. § (3) bekezdés d) pontja

²³ Kormányrendelet 5/B. § c) pontja

- 4.4.7. Az intézmény meghatározza, hogy milyen módon és meddig van lehetőség a korábbi futtatható kód visszatöltésére, illetve a korábbi működés visszaállítására.
- 4.4.8. Az intézmény gondoskodik a megváltoztatott informatikai rendszerek, rendszerelemek, paraméterek éles üzembe állítását megelőző, dokumentált, elvárható gondosságú teszteléséről. A tesztelés során az intézmény gondoskodik a funkcionális és a nem funkcionális tesztek elvégzéséről, beleértve az informatikai biztonsági tesztek is.
- 4.4.9. Az intézmény gondoskodik a fejlesztési és a teszt környezet elkülönítéséről adatbázis és hálózati szinten is.
- 4.4.10. Az intézmény mindenkor gondoskodik arról, hogy a beszerzett vagy fejlesztett informatikai rendszerelemek üzembe helyezésekor azok alapértelmezett jelszavai és biztonsági paraméterei beállításainak megváltoztatása megtörténjen.

4.5. Kiszervezés, tevékenységek kihelyezése

- 4.5.1. Az intézmény a kiszervezett vagy kihelyezett tevékenységért ugyanúgy felel, mint ha azt ön maga végezné, ezért fontos, hogy az adatvédelmi és az információbiztonsági elvek érvényesülésére az intézmény megfelelő garanciákat építsen be a szerződéseibe, és ezek teljesülését megfelelően kontrollálja. A harmadik fél általi adathozzáférésekkel kapcsolatban az intézmény a tevékenység kiszervezéseként való kezelésével biztosítja a szolgáltatás – az intézmény, illetve az MNB általi – megfelelő ellenőrizhetőségét és átlátható működését. Kihelyezett tevékenységen azt a szolgáltatást értjük, amelyeket az intézmény nem maga végez, hanem külső szolgáltatótól vesz igénybe, de a vonatkozó törvényi rendelkezés szerint nem minősül kiszervezésnek²⁴.
- 4.5.2. A kiszervezés vagy kihelyezés során az intézmény gondoskodik arról, hogy az ügyfeladathoz, illetve a pénzügyi ágazati titokhoz hozzáférők számára is megfelelő adminisztratív védelmi kontrollok kerüljenek kialakításra, mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állási normák számonkérhetősége érdekében.
- 4.5.3. A kiszervezett vagy kihelyezett adatkezelés, adatfeldolgozás vagy adattárolás vonatkozásában az intézmény megfelelő garanciális szabályokat határoz meg, amelyek biztosítják, hogy az ügyfél- vagy pénzügyi ágazati titok körébe tartozó adatot csak az adatkezelés céljának megvalósulásához elengedhetetlen mértékben és ideig kezeljen az adat kezelője, továbbá ezek feldolgozását is a célhoz kötöttség elve alapján szabályozza.
- 4.5.4. Kiszervezéskor illetve kihelyezéskor az intézmény gondoskodik az érintettek megfelelő tájékoztatásáról annak érdekében, hogy az ügyfeladat, illetve pénzügyi ágazati titok körébe tartozó adataik vonatkozásában az adatfeldolgozás teljes útja az érintettek számára is követhető és ellenőrizhető legyen.
- 4.5.5. Az intézmény és a kiszervezett vagy kihelyezett tevékenységet végző (szolgáltató) szerződésben rögzítik:
- a) a szolgáltató által minimálisan elkészítendő és betartandó szabályzatokat,

²⁴ A külső szolgáltatók igénybevételéről szóló MNB ajánlás hatálya alá tartozó intézmények esetében ide sorolandók a közvetítői megállapodás és a külső szolgáltatóval kötött egyéb megállapodás alapján ellátott tevékenységek is.

- b) a szolgáltató informatikai biztonsági feladatait és felelősségét, ezen belül a kiszervezett vagy kihelyezett tevékenységekre vonatkozó kockázatelemzés feladatát, valamint annak hatókörét,
- c) az intézmény által elvárt visszaállási pontokat és helyreállítási időket,
- d) a szolgáltató kötelezettségét az üzletfolytonossági tervezés és felkészülés elvégzésére (már a szolgáltatás megkezdését megelőzően),
- e) a szolgáltató felelősségét üzletfolytonossági eljárásainak mindenkor alkalmazhatóságára,
- f) ezen eljárások tesztelésének módszerét, gyakoriságát, valamint az intézmény felé történő beszámolás módját
- g) a szerződés megszűnését követő eljárásokat és átadásokat (eszközök, adatok, adatszerkezetek, folyamatleírások, rendszertervek, dokumentációk, forráskódok, üzleti logikai megoldások), az átadás formátumát, a szerzői és vagyoni jogokat, licenc- és jogdíjakat, valamint az együttműködési kötelezettséget és az ezekkel kapcsolatban felmerült költségek viselését.

4.5.6. Az intézmény minden olyan tevékenysége során, ahol harmadik fél az ügyfél adataihoz vagy az ügyfél közvetett azonosítására vagy hitelesítésére alkalmas adatokhoz bármilyen módon hozzáférhet – függetlenül attól, hogy ezt milyen minőségében és joggal teszi – mérlegeli a kiszervezésre vonatkozó előírások teljesülését.

IV. ÜZEMELTETÉS

5. ADMINISZTRATÍV VÉDELEM

5.1. A működtetésre vonatkozó szabályzatok

5.1.1. Vonatkozó jogszabályi rendelkezés: *az intézménynek rendelkeznie kell az informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal.²⁵ Az intézmény élesüzemi rendszere üzemeltetési folyamatai szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek;²⁶ az élesüzemi rendszer karbantartása szabályozott, és megfelel a rendelkezésre állásra vonatkozó elvárásoknak,²⁷ az élesüzemi rendszer és az üzemeltetési szabályzatok gondoskodnak a rendszerelemek és a kezelt információk sértetlenségéről,²⁸ az élesüzemi rendszer és az üzemeltetési szabályzatok gondoskodnak a rendszer és a kommunikáció kellő szintű védelméről²⁹. A szabályozások és eljárások garantálják a rendszer biztonsági szintjének folyamatos fenntartását, a szoftverek frissítését, üzemeltetését.³⁰*

5.1.2. Az informatikai biztonsági szabályozási rendszer infrastruktúra-közeli operatív utasításai és leírásai nyújtanak szakmai támogatást az informatikai rendszerek megfelelő védelmének naprakész állapotban tartásához, napi üzemének biztosításához, az üzemeltetési, szolgáltatásfolytonossági feladatok

²⁵ Bszt. 12. § (7) bekezdés a) pontja, Mpt. 77/A. § (6) bekezdés a) pontja, Öpt. 40/C. § (6) bekezdés a) pontja, Kormányrendelet 3. § (3) bekezdés a) pontja

²⁶ Kormányrendelet 5/B. § b) pontja

²⁷ Kormányrendelet 5/B. § m) pontja

²⁸ Kormányrendelet 5/B. § o) pontja

²⁹ Kormányrendelet 5/B. § p) pontja

³⁰ Kormányrendelet 5/A. § (3) bekezdés c) pont cd) alpontja

megfelelő ellátásához, valamint a katasztrófahelyzetet követő hatékony helyreállításhoz. A fenti feladatok ellátását az intézmény az alábbi elvárások teljesítésével támogatja.

- 5.1.3. Az intézmény az informatikai rendszer napi működtetésére vonatkozó operatív utasításai, műszaki- és nyilvántartási dokumentumai, feljegyzései (a továbbiakban együtt: operatív utasítások) elkészítését, dokumentálását és felülvizsgálatát az informatikai biztonsági szabályozási rendszerben szabályozza.
 - 5.1.4. Az MNB elvárja, hogy az operatív utasítások együttesen alkalmasak legyenek arra, hogy egy, a területen jártas szakértő az adott üzemeltető vagy szolgáltató elérhetetlensége esetén is képes legyen biztosítani a rendszer folyamatos üzemét vagy helyreállítását.
 - 5.1.5. Az operatív utasítások biztosítják, hogy egy független informatikai vizsgálat meggyőződhessen a tevékenység tartalmának megfelelőségéről, és ellenőrizhesse, hogy a tevékenységet az intézmény megfelelően látja-e el.
 - 5.1.6. Az intézmény az informatikai rendszer bevezetéséhez elkészíti, majd változások esetén, de legkésőbb a kockázatelemzés felülvizsgálata keretében felülvizsgálja, és aktualizálja legalább az alábbi operatív utasításait:
 - a) futtató környezetek rendszerenkénti leírása (működési architektúra, működtető környezetek, adatbázis kezelő, felügyeleti megoldások bemutatása),
 - b) a rendszerek üzemeltetési leírásai: a rendszeres üzemeltetői és ellenőrzési tevékenységek előírása, a naplók ellenőrzési feladatai, a feladat végrehajtásához rendelt beszámolók, feljegyzések készítése, nyilvántartások vezetése.
 - 5.1.7. Az intézmény gondoskodik arról, hogy a szolgáltatás-folytonosság biztosítása érdekében az operatív utasítások – megfelelő (fizikai és logikai) hozzáférés-védelem kialakítása mellett – a tartalék (székhelytől, illetve fő telephelytől eltérő) helyszínen is tárolásra kerüljenek.
 - 5.1.8. Az intézmény megfontolja, és kockázataival arányosan dönt az egyes rendszerek beállítási és telepítési leírásainak elkészítéséről, illetve ezek informatikai biztonsági szabályozási rendszerbe illesztéséről.
- 5.2. Szoftvereszközök nyilvántartása
- 5.2.1. Vonatkozó jogszabályi rendelkezés: *az intézménynél mindenkor rendelkezésre kell állnia az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.*³¹
 - 5.2.2. Az intézmény meghatározza az egyes eszközökre telepíthető szoftverek és szoftververziók körét, és biztosítja, hogy az egyes eszközökön csak engedélyezett szoftverek legyenek telepítve.
 - 5.2.3. Az intézmény biztosítja, hogy valamennyi ügyviteli, üzleti szoftvereszközének (legalább a szolgáltatásnyújtáshoz kapcsolódó alapszoftverek, alkalmazási rendszerek, adatbázis-kezelők) teljes körű nyilvántartása informatikai rendszereiből bármikor azonnal előállítható, vagy – ennek hiányában – ezekről teljes körű, naprakész nyilvántartást vezet.
 - 5.2.4. A nyilvántartás a számviteli nyilvántartással megfeleltethető, tartalmazza az intézmény azon eszközein lévő szoftvereket is, amelyek az adott hálózathoz nem érhetők el.
 - 5.2.5. Előremutató gyakorlat

³¹ Bszt.12. § (9) bekezdés g) pont, Mpt. 77/A. § (7) bekezdés g) pont, Öpt. 40/C. § (7) bekezdés g) pont, Kormányrendelet 4. § (1) bekezdés g) pont

A pénzügyi szervezet megfontolja, és kockázatai arányában dönt önálló szoftver nyilvántartás bevezetéséről, és a nyilvántartást rendszeres időközönként összeveti az informatikai eszközein telepített szoftvereivel.

5.3. Az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződések

5.3.1. Vonatkozó jogszabályi rendelkezés: *a pénzügyi intézménynél mindenkor rendelkezésre kell állnia az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek.*³²

5.3.2. Az intézmény rendelkezik az általa birtokolt, illetve használt szoftver eszközök jogtisztaságát igazoló bizonylatokkal - szerződések, licenc számlák, licencigazolások stb. –, és ezeket oly módon tárolja, hogy egy, a jogtisztaságra vonatkozó belső vagy külső ellenőrzés bármikor azonnal elvégezhető legyen.

5.3.3. Az intézmény rendszeresen ellenőrzi, hogy az eszközeire telepített szoftverek – beleértve a szoftververziókat – a licencekben foglaltaknak megfelelően kerülnek felhasználásra.

5.4. Az informatikai rendszer elemeinek azonosítása

5.4.1. Vonatkozó jogszabályi rendelkezés: *az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról.*³³ *Az intézmény biztosítja, hogy az élesüzemi rendszer elemei azonosíthatóak és dokumentáltak.*³⁴

5.4.2. Az intézmény a saját, illetve az általa használt eszközeiről – ideértve az informatikai és adatkommunikációs működéshez kapcsolódó hardver és szoftver eszközöket, rendszerelemeket, személyi hitelesítő eszközöket stb. – műszaki célú nyilvántartást vezet, amely rögzíti legalább az alábbiakat:

- a) az eszköz pontos megnevezése, típusa, egyedi azonosítója,
- b) az eszköz aktuális, pontos elhelyezése – tárolási helye, vagy mobil eszközök esetében a használó személye,
- c) az eszköz hardver és szoftver konfigurációja
- d) az eszköz tulajdonosa, használója, felelőse.

5.4.3. A nyilvántartás mindenkor naprakész, a számviteli nyilvántartással megfeleltethető, tartalmazza az intézmény azon eszközeit is, amelyek az adott hálózatból nem érhetők el.

5.4.4. Az intézmény a kritikus üzemeltetési helyszíneire belépési jogosultsággal rendelkező személyeket azonosítja, és a belépéseket nyilvántartja.

6. FIZIKAI VÉDELEM

6.1. Vonatkozó jogszabályi rendelkezés:

³² Bszt. 12. § (9) bekezdés f) pontja, Mpt. 77/A. § (7) bekezdés f) pontja, Öpt. 40/C. § (7) bekezdés f) pontja, Kormányrendelet 4. § (1) bekezdés f) pontja

³³ Bszt. 12. § (6) bekezdés a) pontja, Mpt. 77/A. § (5) bekezdés a) pontja, Öpt. 40/C. § (5) bekezdés a) pontja, Kormányrendelet 3. § (2) bekezdés a) pontja

³⁴ Kormányrendelet 5/B. § a) pontja

az intézmény kiépíti az informatikai rendszere biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működteti,³⁵ megfelelő szintű fizikailag védett környezetet biztosít az élesüzemi rendszer számára³⁶.

6.2. Általános elvárások:

A szolgáltatásfolytonosság valamint az adatok bizalmosságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében az adminisztratív és a logikai biztonságon felül az MNB elvárja, hogy az intézmény gondoskodjon a kritikus infrastruktúra elemek fizikai hozzáférés-védelméről, a hozzáférések utólagos ellenőrizhetőségéről, valamint a nem üzemszerű környezeti tényezők folyamatos ellenőrzéséről, hatásaik kiküszöböléséről, korrigálásáról. Ennek érdekében az intézmény legalább az alábbi védelmi intézkedésekről gondoskodik:

6.2.1. Az intézmény megfelelő szervezési, szabályozási, fizikai és technológiai kontrollok kialakításával biztosítja, hogy a kritikus infrastruktúra elemeket (informatikai hálózati és kiszolgáló eszközöket, rendszereket, informatikai biztonságot szolgáló megoldásokat) koncentráltan tartalmazó helyiségekben vagy tárolókban lévő eszközökhöz csak az arra kifejezetten jogosult személyek, ellenőrzött és naplózott módon férhessenek hozzá (például beléptető rendszer, megfelelő falazat és ráncszós kialakítása).

6.2.2. Az intézmény gondoskodik a kritikus infrastruktúra elemeket tartalmazó helyiségek környezeti paramétereinek folyamatos figyeléséről és ellenőrzéséről, nem üzemi körülmények észlelésekor a kijelölt felelősök azonnali riasztásáról legalább az alábbiak esetén:

- a) tápáramellátás (akadozás, ingadozás, kimaradás),
- b) üzemtől eltérő hőmérséklet,
- c) magas páratartalom,
- d) füst, tűz,
- e) nedvesség, víz,
- f) nyílászárók indokolatlan nyitása és nyitva tartása,
- g) indokolatlan mozgások.

6.2.3. Az intézmény a kockázatokkal arányosan gondoskodik a kritikus infrastruktúra elemeket tároló helyiségek 6.2.2. pontban meghatározott környezeti paramétereinek vonatkozásában az üzemtől eltérő működést eredményező események megakadályozásáról (például, de nem kizárólag tűz- és behatolásvédelmi rendszerek kialakításával).

6.2.4. Az intézmény a kockázatelemzésében kitér a helyiségek megfelelő tűzzáró falazattal és nyílászárókkal történő ellátásának szükségességére és megvalósítására.

6.2.5. Az intézmény gondoskodik a tápáramellátás folyamatos biztosításáról mind a rövid, mind a hosszú távú áramkimaradások esetére.

6.2.6. Az intézmény gondoskodik a megfelelő üzemi hőmérséklet folyamatos biztosításáról.

6.2.7. Az intézmény gondoskodik a fizikai védelmi és ellenőrző berendezések és eszközök folyamatos karbantartásáról, valamint működőképességük ellenőrzéséről.

³⁵ Bszt. 12. § (5) bekezdése, Mpt. 77/A. § (4) bekezdése, Öpt. 40/C. § (4) bekezdése, Kormányrendelet 3. § (1) bekezdése

³⁶ Kormányrendelet 5/B. § q) pontja

6.2.8. Előremutató gyakorlat

- a) Az intézmény a kockázataival arányosan gondoskodhat arról, hogy a kritikus infrastruktúra elemeket koncentráltan tartalmazó helyiségek és tárolók fizikai hozzáférés-védelmének ellenőrző rendszerét az adatvédelmi előírások betartása mellett kamerás megfigyelő és rögzítő rendszerrel is kiegészíti.
- b) Az intézmény a kockázataival arányosan gondoskodhat arról, hogy a kritikus infrastruktúra elemeket koncentráltan tartalmazó helyiségek tűzvédelmét automata tűzoltó berendezéssel is kiegészíti.

7. Hálózati védelem

7.1. Vonatkozó jogszabályi rendelkezés:

a pénzügyi intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről...³⁷ Az intézmény biztosítja, hogy az élesüzemi rendszer adatkommunikációs és rendszerkapcsolatai dokumentáltak és ellenőrzöttek annak érdekében, hogy az adatkommunikáció bizalmassága, sértetlensége és hitelessége biztosítható legyen³⁸, a szervezet detektálja és kezeli az egyes biztonsági eseményeket.³⁹ Az informatikai rendszer összes külső interfésze szabályozott és kontrollált.⁴⁰

7.2. Általános elvárás:

Elvárás, hogy az adatkommunikációs, rendszerkapcsolati és hálózati dokumentációknak együttesen alkalmasak legyenek az üzleti folyamatok adatáramlásainak nyomon követésére, a folyamatot támogató kapcsolatok (interfészek) és eszközök azonosítására. Az így azonosított eszközökre és kapcsolatokra alkalmazandók az adatbesorolás alapján indokolt védelmi intézkedések, biztosítva, hogy a kommunikációs közegben az adatok hitelesek maradnak, és nem sérül azok bizalmassága és integritása.

7.3. Adatkommunikációs rendszerek dokumentálása

7.3.1. Az intézmény a szabályozási rendszerében meghatározottak alapján gondoskodik az adatkommunikációs, rendszerkapcsolati dokumentáció és a hálózatmenedzsment operatív utasítások elkészítéséről és felülvizsgálatáról.

7.3.2. Az intézmény biztosítja, hogy az adatkommunikációs rendszerének dokumentációja alkalmas az egyes üzleti folyamatok infrastrukturális – adatkapcsolati és hálózati szintű – nyomon követésére. Ennek érdekében rendelkezik legalább az alábbi dokumentumokkal:

- a) az eszközök, rendszerek, szerelemek azonosíthatóságát, a közöttük lévő kapcsolatok típusát és jellegét, azonosíthatóságát is feltüntető adatkapcsolati ábra,
- b) az adatkapcsolati ábrával összevethető hálózati topológia ábra,

³⁷ Bszt. 12. § (6) bekezdés e) pontja, Mpt. 77/A. § (5) bekezdés e) pontja, Öpt. 40/C. § (5) bekezdés e) pontja, Kormányrendelet 3. § (2) bekezdés e) pontja

³⁸ Kormányrendelet 5/B. § j) pontja

³⁹ Kormányrendelet 5/B. § r) pontja

⁴⁰ Kormányrendelet 5/A. § (3) bekezdés c) pont cc) alpontja

- c) géptermi elhelyezési rajzok,
- d) hálózati zónák és átjárási szabályok leírása.

7.4. Az adatok védelme távadatátvitel során

7.4.1. Az intézmény a felhasználók vagy az ügyfelek azonosítására, vagy hitelesítésére alkalmas, illetve pénzügyi ágazati titok körébe tartozó adatot, távoli hálózaton – ideértve a bérelt vonalakkal kiépített magánhálózatokat is – csak rejtjelezett formában továbbít.

7.4.2. Az intézmény jelszavakat vagy más hitelesítő adatokat távoli és lokális hálózaton is csak rejtjelezett formában továbbít.

7.4.3. Az intézmény kockázati szempontból kritikus pontoknak minősíti azokat a vezeték nélküli hálózatokat, adatátviteli módokat és ezeket használó eszközöket (például WiFi, Bluetooth, mobil kommunikációs eszközök), amelyeken ügyfeladatot vagy pénzügyi ágazati titok körébe tartozó adatot továbbíthat, illetve amelyek az intézmény adathálózatára csatlakoznak.

7.4.4. Az intézmény az informatikai rendszeréhez engedélyezett távelérés, vagy hordozható eszközökkel történő csatlakozás biztonsága érdekében megteszi legalább az alábbi biztonsági intézkedéseket:

- a) Az intézmény a belső hálózatán lévő informatikai rendszereihez (beleértve a virtuális privát hálózati vagy levelező rendszereket is) történő csatlakozást csak engedélyezett felhasználók és eszközök számára, csak központi megoldáson keresztül, csak a szükséges mértékig és a szükséges eszközök eléréséhez biztosítja.
- b) Az intézmény az eszközökön megköveteli és technológiailag is kikényszeríti legalább a következő biztonsági beállítások alkalmazását: titkosítás, automatikus képernyőzárolás, a képernyőzár feloldásához legalább 5 jegyű PIN kód, vagy ennél biztonságosabb megoldás, adatszivárgás elleni védelem, kétfaktoros autentikáció, korlátozott adatelérés, távoli törlés.
- c) Az intézmény a biztonsági szempontok figyelembevételével meghatározza és technológiailag kikényszeríti azokat a minimum követelményeket (legalább a hardver, az operációs rendszer és a kapcsolódó alkalmazások szintjén), amelynél korábbi verziókat nem alkalmazhat a kapcsolathoz. Az eszközökben tiltja a felhasználók adminisztrátori szintű hozzáférését, valamint a feltört eszközök használatát (rootolt, jailbreakelt).
- d) Virtuális privát hálózatok esetén az intézmény a kapcsolódáshoz titkosítási és integritási algoritmusokat, autentikációs metódusokat és protokollokat, valamint biztonsági szempontú technikai validációt alkalmaz (így például, de nem kizárólag a távoli kliens vírusvédelmének megfelelése, a telepített biztonsági javítócsomagok megfelelése, lokális tűzfal használata, osztott elérés – split tunneling – tiltása, a lemez titkosítás, vagy az adatszivárgás elleni védelmi megoldás megléte).
- e) Az intézmény tiltja, vagy csak a megfelelő kontrollokkal, a kockázatokkal arányosan engedélyezi a felhasználói saját eszközök (BYOD) kapcsolódását az informatikai infrastruktúrájához, ennek során megköveteli legalább az a), b) és c) pontban meghatározottak kikényszerítését.
- f) Az intézmény gondoskodik a távelérések folyamatos monitorozásáról, valamint a biztonsági események - lehetőség szerinti automatikus - észleléséről és kezeléséről.
- g) Az intézmény gondoskodik a távelérési szabályainak és beállításainak, felhasználói körének folyamatos felülvizsgálatáról és frissítéséről.

- h) Az intézmény biztosítja a távoli eléréseket kezelő védelmi rendszer hibatűrését, rendelkezésre állását a konfigurációjának mentését, a lényeges eseményeinek naplózását és központi naplógyűjtését és -kiértékelését.

7.4.5. Az intézmény kritikus adatai hálózati átvitele során biztosítja az adatok bizalmasságát, sértetlenségét és hitelességét, valamint ezen kritériumok teljesülésének ellenőrizhetőségét.

7.5. Határvédelem

7.5.1. Az MNB elvárja, hogy a hálózati kapcsolatok – beleértve a hálózati szegmensek közötti átjárásokat – úgy kerüljenek kialakításra, hogy azokon mindenkor csak az üzletileg indokolt és engedélyezett forgalom haladjon át.

7.5.2. Az intézmény gondoskodik a megfelelően szabályozott, üzleti igényekkel alátámasztott, engedélyezett, dokumentált, azonosítható és rendszeresen – de legkésőbb a kockázatelemzés felülvizsgálata során – felülvizsgált hálózati kapcsolati szabályrendszerrel.

7.5.3. Az intézmény az engedélyezett kommunikációs, kapcsolati szabályokat megfelelő, az egyes hálózati rétegekben a kockázatokkal arányos védelmet biztosító határvédelmi megoldások (például tűzfal, behatolás megelőző rendszer, alkalmazásszintű tűzfal, WEB- és e-mail tartalomszűrő, adatszivárgás elleni védelmi rendszer) használatával technológiailag is kikényszeríti, és a kockázatokkal arányosan többszintű védelmet biztosít a külső támadásokkal szemben. A határvédelmi megoldás túlterhelése vagy meghibásodása esetén a kapcsolatokat lezárja. Az internetes hálózati környezet határvédelme során az intézmény a kockázataival arányosan a magasabb szintű hálózati (applikációs) rétegekben is rendelkezik megfelelő megoldásokkal a hálózati tartalmak monitorozására, a nem megfelelő tartalmak kiszűrésére, valamint a webes alkalmazásai védelmére. A külső kapcsolatai vonatkozásában ellenőrzi a titkosított adatforgalmat is.

7.5.4. Az intézmény gondoskodik a nem kívánt hálózati kapcsolatok és események automatikus kiszűréséről.

7.5.5. Az intézmény gondoskodik az adatszivárgás kockázatokkal arányos megakadályozásáról. Ennek keretében legalább:

- a) az informatikai biztonsági szabályozási rendszerében részletesen szabályozza az adatszivárgással összefüggő üzemeltetési feladatokat és felelőségeket, különösen az adminisztrátori hozzáférések és az adatszivárgási incidensek kezelésének feltételeit;
- b) a szabályozási rendszerben meghatározott rendszerességgel, de legkésőbb a kockázatelemzés felülvizsgálatkor hálózati felderítést végez az érzékeny adatok tárolási helyeinek azonosítására;
- c) a potenciális adatszivárgási csatornák felügyeletére a kockázatokkal arányos védelmi, monitorozási megoldásokat alkalmaz legalább a webes hozzáférés, az e-mail kapcsolat, a végpontok, a hordozható eszközök, a fájlszerverek, a felhő szolgáltatások és a nyomtatók alkalmazása vonatkozásában;
- d) a felhasználók számára tiltja, vagy a megfelelő kontrollok bevezetése mellett – így például külön jogosultsághoz, adattartalom ellenőrzéshez, adatszivárgási technológiai megoldáshoz stb. kötve – korlátozza a külső adathordozók használatát;
- e) a kockázatokkal arányosan tiltja, és technológia alkalmazásával szűri a potenciális adatszivárgási kockázatot vagy kártékony kódokat hordozó internetes tartalmakhoz való hozzáférést – legalább a webmail, online tárolók, peer-to-peer tartalmak vonatkozásában. A kockázatos tartalmak szűréséhez dinamikusan frissülő URL listákat is használ;

- f) a biztonsági kockázatokkal arányos módon az adatszivárgás kockázatának kezelésére átfogó, a potenciális adatszivárgási csatornákat központilag felügyelő adatszivárgás védelmi folyamatokat támogató megoldást (Data Loss Prevention (DLP)) üzemeltet.

7.5.6. Az intézmény felméri és kezeli az adatátviteli hálózaton megvalósított hangátviteli és multimédiás megoldásainak (például VoIP, SIP) határvédelmét és egyéb biztonságát érintő kockázatait.

7.5.7. Az intézmény gondoskodik

- a) a szabályok, szabályrendszerek, határvédelmi eszközök és -szoftvertermékek folyamatos felülvizsgálatáról és tervezett, illetve
- b) a támadási minták, források, URL listák automatikus frissítéséről.

7.5.8. A külső internetes hozzáférések vonatkozásában az intézmény a kockázatokkal arányosan gondoskodik a szolgáltatásai, szerverei, hálózati eszközei leállását vagy lassulását előidéző sávszélesség-, kapcsolatalapú- és alkalmazásszintű túlterheléses támadásokkal szembeni többszintű védelmi megoldásról.

7.5.9. Az intézmény az internetes hálózati környezet felől elérhető eszközei – például a kommunikációs szerverei és webkiszolgálói – védelme érdekében gondoskodik arról, hogy a kiszolgáló szerverek az ún. Demilitarizált Zónában (DMZ), míg az internetes szolgáltatáshoz tartozó web szerverek, a pénzügyi alkalmazások és az adatbázisok a DMZ mögötti, védett belső hálózatokon kerüljenek elhelyezésre.

7.6. Biztonsági események kezelése

7.6.1. Az intézmény gondoskodik a feltárt biztonsági események (incidensek) dokumentált kezeléséről és azok tanulságainak visszacsatolásáról.

7.6.2. Az intézmény nyilvántartást vezet az informatikai rendszerek és rendszerelemek üzemszerű működését akadályozó incidensekről és azok megoldásáról.

7.6.3. Az intézmény gondoskodik a védelmi rendszer folyamatos monitorozásáról a támadások mielőbbi - lehetőség szerint automatikus - észleléséről és kezeléséről.

7.6.4. Az intézmény rendelkezik dokumentált incidenskezelési eljárással, amely tartalmazza legalább az alábbiakat:

- a) szerepek, feladatok, kommunikációs és kapcsolatfelvételi eljárások a hatóságokkal, a felügyeleti szervekkel közvetlen érintettség esetén az ügyfelekkel egy vélt vagy valós támadás, sérülés esetében,
- b) részletes gyakorlati eljárások a szokásos incidensek kezelésére (például a felügyeleti rendszerek riasztásaira, DDoS támadások esetére stb.),
- c) tesztelési eljárások az incidenskezelés megfelelőségének ellenőrzésére.

7.6.5. Az intézmény legkésőbb a kockázatelemzés felülvizsgálatakor, dokumentáltan felülvizsgálja az incidenskezelési eljárásainak megfelelőségét.

7.7. Vírusok és más rosszindulatú kódok elleni védelem

7.7.1. Vonatkozó jogszabályi rendelkezés: *az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell a rendszer biztonsági*

kockázattal arányos vírus- és más rosszindulatú program elleni védelméről.⁴¹ Az intézménynél az élesüzemi rendszer vírus és más rosszindulatú programok elleni védelme biztosított.⁴²

- 7.7.2. Az intézmény az informatikai rendszere elemein a vírusok és más rosszindulatú kódok kiszűrésére alkalmas programot működtet, valamint biztosítja a program, illetve az adatbázisok és minták naprakész állapotát és naplózását.
- 7.7.3. Az intézmény biztosítja a vírusok és más rosszindulatú kódok elleni védelmi rendszere automatikus frissítését, valamint a teljes ellenőrzések (full scan) rendszeres időszakonként – de legalább heti egy alkalommal – történő elvégzését. A teljes ellenőrzések megfelelő kontrollok mellett, egyenértékű megoldásokkal kiválthatók.
- 7.7.4. Az intézmény gondoskodik arról, hogy a vírus és más rosszindulatú programok elleni védelmi rendszer beállításai csak az informatikai biztonsági szabályozási rendszerben meghatározott feltételek és eljárásrend szerint legyenek módosíthatók.
- 7.7.5. Az intézmény gondoskodik arról, hogy a kockázatosnak ítélt állományok csak a megfelelő szakértői ellenőrzéseket és a potenciális veszély elhárítását követően kerülhessenek a végfelhasználókhoz.
- 7.7.6. Az intézmény az Internetelérés és az elektronikus levelezés során a titkosított kapcsolatok vonatkozásában is biztosítja a kártékonykód ellenőrzéseket.
- 7.7.7. Az intézmény gondoskodik arról, hogy az informatikai rendszereiben csak olyan szoftvertermékeket és rendszerprogramokat futtasson, amelyek rendelkeznek terméktámogatással és biztonsági frissítéssel. Gondoskodik továbbá a frissítések rendszeres teszteléséről és élesüzembe állításáról, ezzel is csökkentve az ismert szoftverhiányosságok kihasználásával történő rosszindulatú kódok bejuttatásának kockázatát.
- 7.7.8. Az intézmény a kockázataival arányosan többrétegű, mélységi védelemmel rendelkezik, és központi kezelő felülettel rendelkező végponti biztonsági programot működtet.
- 7.8. Elektronikus levelezés védelme
- 7.8.1. Az intézmény az informatikai biztonsági szabályozási rendszerében rendelkezik az elektronikus levelezés biztonságának szabályairól, eljárásairól.
- 7.8.2. Az intézmény többszintű (központi és végponti), illetve több funkciójú (kéretlen levélszemét, káros kódokat vagy hivatkozásokat tartalmazó levelek, adathalász levelek, adatszivárgásra utaló levelek stb. elleni) védelmet biztosít az internetes levelezésének biztonsága érdekében. Ennek során gondoskodik arról, hogy minden levél – beleértve a titkosított tartalmú vagy titkosított csatolmányokat tartalmazó leveleket is – a központi levélvédelmi megoldások használatával ellenőrzésre és indokolt esetben szűrésre kerüljön.
- 7.8.3. Az intézmény csak az üzletileg indokolt, technikailag szükséges eszközök, hálózati szegmensek és személyek számára engedélyezi az elektronikus levelezést.
- 7.8.4. Az intézmény az elektronikus levelezése során az adatok bizalmosságának védelme érdekében titkosított adatkapcsolaton keresztül biztosítja a levélküldés és -fogadás lehetőségét, illetve a levél adattartalmának függvényében a kockázatokkal arányosan gondoskodik a levelek adattartalmának titkosításáról is.

⁴¹ Bszt. 12. § (6) bekezdés g) pontja, Mpt. 77/A. § (5) bekezdés g) pontja, Öpt. 40/C. § (5) bekezdés g) pontja, Kormányrendelet 3. § (2) bekezdés g) pontja

⁴² Kormányrendelet 5/B. § i) pontja

- 7.8.5. Az intézmény folyamatosan gondoskodik az elektronikus levelezőrendszere biztonsági beállításainak megfelelőségéről, tiltja az ellenőrizetlen forrásból származó levelek rendszeren keresztül történő elküldését vagy továbbítását. Az intézmény folyamatos ellenőrzés mellett gondoskodik a levelező rendszer megfelelő Domain Name System (DNS) beállításairól is.
- 7.8.6. Az intézmény a kockázataival arányosan elkülöníti (karanténba helyezi) a kéretlen vagy potenciális kockázatokkal járó leveleket. Gondoskodik arról, hogy a kockázatos levelek és tartalmak megfelelő szakmai ellenőrzés és szűrés nélkül ne kerüljenek a végfelhasználókhoz.
- 7.8.7. Az intézmény gondoskodik az alkalmazott védelmi rendszer szabályainak, beállításainak, szignatúráinak folyamatos felülvizsgálatáról és frissítéséről.
- 7.8.8. Az intézmény a kockázatokkal arányosan biztosítja a védelmi rendszer folyamatos monitorozását, a hibatűrését, a rendelkezésre állását, a konfigurációjának mentését, a lényeges és biztonsági eseményeinek naplózását, központi naplójújtását, a naplók kiértékelését és szükség esetén automatikus riasztását.

8. LOGIKAI VÉDELEM

8.1. Logikai védelemre vonatkozó közös rendelkezések

8.1.1. Vonatkozó jogszabályi rendelkezés: *A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról: [...] b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljességét biztosító [...] eljárásokról,⁴³ A szoftvereknek együttesen alkalmasnak kell lenniük [...] a biztonsági kockázattal arányos logikai védelemre és a sérthetlenség védelmére⁴⁴.*

8.2. Adatbázisok biztonsága

8.2.1. Az intézmény az informatikai biztonsági szabályozási rendszerében meghatározza az adatbázisok üzemeltetésére és védelmére vonatkozó szabályokat és eljárásokat.

8.2.2. Az intézmény tiltja a közvetlen adatbázis-hozzáféréseket. A kivételes eseteket egyenként engedélyeztetni, ezek során kiemelt figyelmet fordít az adatbázisok és az adatbázisokban található adatok közvetlen módosításainak kezelésére, felügyeletére és a tevékenységek megfelelő naplózására. Ennek folyamatát az informatikai biztonsági szabályozási rendszerében szabályozza, és mindenkor gondoskodik arról, hogy a tevékenység végzését független személy vagy szervezet folyamatosan kontrollálja.

8.2.3. Az intézmény az adatbáziskezelő rendszerek biztonsági beállításait a gyártói és a vonatkozó szakmai ajánlások alapján rendszeres időközönként felülvizsgálja, és a kockázatokkal arányosan meghatározza és kikényszeríti az adatbázis konfigurációs- és a biztonsági paraméterek erősítésére szolgáló hardening elvárásokat, beleértve az adatbázisok biztonsági paramétereit, felhasználó- és jelszó követelményeit, naplózási és auditing beállításait.

⁴³ Bszt. 12. § (6) bekezdés b) pontja, Mpt. 77/A. § (5) bekezdés b) pontja, Öpt. 40/C. § (5) bekezdés b) pontja Kormányrendelet 3. § (2) bekezdés d) pontja

⁴⁴ Bszt. 12. § (10) bekezdés f) pontja, Mpt. 77/A. § (8) bekezdés c) pontja, Öpt. 40/C. § (8) bekezdés c) pontja, Kormányrendelet 4. § (2) bekezdés e) pontja

8.2.4. Az intézmény gondoskodik az adatbázisok működésének folyamatos monitorozásáról, valamint az események - lehetőség szerint automatikus - észleléséről és kezeléséről.

8.2.5. Az intézmény a kockázatokkal arányosan biztosítja az adatbázisrendszerek hibatűrését, rendelkezésre állását, a konfigurációk és az adatbázisok mentését, a lényeges eseményeinek naplózását és központi naplógyűjtését és -kiértékelését.

8.2.6. Az intézmény a biztonsági kockázatokkal arányosan adatbázis titkosítást alkalmaz, és gondoskodik a titkosításhoz szükséges kulcsok biztonságos kezeléséről.

8.3. Virtuális környezetek biztonsága

8.3.1. Az intézmény az informatikai biztonsági szabályozási rendszerében meghatározza az alkalmazott virtuális környezetek üzemeltetésére és védelmére vonatkozó szabályokat és eljárásokat.

8.3.2. Az intézmény az informatikai rendszerében alkalmazott virtuális környezeti rendszerek biztonsági beállításait a gyártói és vonatkozó szakmai ajánlások alapján felülvizsgálja, és a kockázatokkal arányosan meghatározza és kikényszeríti a konfigurációs- és a biztonsági paraméterek erősítésére szolgáló hardening elvárásokat. Gondoskodik az alkalmazott virtuális környezeteihez kiadott gyártói frissítések rendszeres telepítéséről.

8.3.3. Az intézmény gondoskodik a virtuális környezeti rendszerelemek működésének folyamatos monitorozásáról, illetve az események - lehetőség szerinti automatikus - észleléséről és kezeléséről.

8.3.4. Az intézmény a kockázatokkal arányosan biztosítja a virtuális rendszerek hibatűrését, rendelkezésre állását, a konfigurációk és a virtuális eszközök biztonsági mentését, a rendszerelemeket érintő lényeges eseményeinek naplózását, központi naplógyűjtését és kiértékelését. A biztonsági kockázatokkal arányosan kialakítja és naprakészen tartja a virtuális eszközök telepítéséhez szükséges állományokat.

8.3.5. Az intézmény a kockázatokkal arányosan gondoskodik a virtuális eszközök (virtuális guest-ek, diszkek) titkosításáról, és a titkosításhoz szükséges kulcsok biztonságos kezeléséről.

8.4. Adatátadások

8.4.1. Az intézmény gondoskodik arról, hogy a rendszerei, illetve a rendszerelemei közötti adatátadások automatikus módon, szabványos interface-eken történjenek. Az intézmény tiltja, illetve a meglévő adatátadások vonatkozásában ütemezetten kivezeti a manuális vagy fájl alapú adatátadásokat. A kivezetés során is folyamatosan gondoskodik az adatok bizalmosságának, sértetlenségének és rendelkezésre állásának megőrzéséről.

8.4.2. Az intézmény üzleti döntéseinek meghozatalában, az adatszolgáltatásokban és az ügyfelek adatainak kezelésében szerepet játszó adatok és folyamatok kezelésére mindenkor olyan informatikai rendszereket használ, amelyek vonatkozásában biztosíthatók az informatikai biztonsági zárttsági feltételek. Az intézmény ezen folyamataiban tiltja az irodai alkalmazáscsomagokkal vagy magasszintű fejlesztői eszközökkel, illetve más módon történő egyedi felhasználói adatelőállítás, kivéve, ha azt jogszabály vagy hatósági eljárás írja elő, vagy az intézmény megfelelő kiegészítő kontroll megoldásokkal biztosítja az alapvető zárttsági feltételek teljesülését.

9. HOZZÁFÉRÉSI REND

9.1. Vonatkozó jogszabályi rendelkezés:

Az intézménynél az élesüzemi rendszerhez való végfelhasználói hozzáférés mind alkalmazási, mind pedig infrastruktúra szinten szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött.⁴⁵ Az intézménynél mindenkor rendelkezésre kell állnia az adatokhoz történő hozzáférési rend meghatározásának,⁴⁶ valamint az intézménynek gondoskodnia kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.⁴⁷ A jogosult általános (emberek és program entitások) és privilegizált (speciális jogokkal felruházott) felhasználók – így különösen rendszergazdák – kizárólag a szigorúan szabályozott szerepköröknek megfelelően férhetnek a védendő információkhoz és az azokat kezelő rendszer elemeihez, kezdeményezhetnek aktivitásokat, valamint kizárólag meghatározott privilegizált felhasználók adhatnak szabályozott szerepköröknek megfelelően és ellenőrzött módon hozzáférési jogosultságokat.⁴⁸

9.2. Hozzáférési rend szabályozása

9.2.1. Az intézmény a szükséges legkevesebb jogosultság elve alapján meghatározza és dokumentálja az üzleti és informatikai szerepkörökhöz tartozó hozzáférési szabályokat. Ennek során az intézmény teljesszűrtően meghatározza és dokumentálja azokat a szerepköröket, amelyek egymással összeférhetetlenek.

9.2.2. Az intézmény az informatikai biztonsági szabályozási rendszerében rendelkezik az informatikai rendszerekhez történő hozzáférés szabályozásáról.

9.2.3. Az intézmény az informatikai rendszerében technológiai megoldásokkal kikényszeríti a hozzáférési szabályok érvényesülését, beleértve az összeférhetetlen szerepkörök egyidejű alkalmazásának kizárását.

9.3. Az adatokhoz való hozzáférés rendje

9.3.1. A hozzáférési rend rögzíti mindazokat a rendszerváltozókat és beállítási értékeket, amelyek meghatározzák, hogy az adatokhoz csak az arra jogosultak, és ők is csak a számukra elengedhetetlenül szükséges műveletek elvégzése céljából férjenek hozzá. Az egyes rendszerek hozzáférési rendjét a rendszerek műszaki dokumentációja vagy önálló dokumentum tartalmazza.

9.3.2. Az intézmény az adatokhoz való hozzáférési rendjét az informatikai biztonsági szabályozási rendszerében szabályozza.

9.3.3. A hozzáférések kezelése során az intézmény azonosítja azokat a jogosultsági objektumokat és erőforrásokat, amelyekhez az informatikai rendszerben definiált felhasználók (fiókok) hozzáférhetnek, és amely felhasználókat folyamatok (például processzek, tárolt eljárások, automatizált tevékenységek) vagy személyek (például munkavállalók, beszállítók, partnerek, ügyfelek) megszemélyesítik.

9.3.4. Az intézmény a jogosultsági objektumokat és erőforrásokat kockázataik szerint minősíti és csoportosítja. Az intézmény a felhasználói (fiók) hozzáférések módját és szabályait a csoportosítással összhangban állapítja meg.

9.3.5. Az intézmény a jogosultsági objektum és erőforrás, a felhasználó (fiók) és a megszemélyesítő összerendeléseket mindenkor nyilvántartja.

⁴⁵ Kormányrendelet 5/B. § e) pontja

⁴⁶ Bszt. 12. § (9) bekezdés d) pontja, Mpt. 77/A. § (7) bekezdés d) pontja, Öpt. 40/C. § (7) bekezdés d) pontja, Kormányrendelet 4. § (1) bekezdés d) pontja

⁴⁷ Bszt. 12. § (8) bekezdése, Mpt. 77/A. § (6) bekezdés e) pontja, Öpt. 40/C. § (6) bekezdés e) pontja, Kormányrendelet 3. § (4) bekezdése

⁴⁸ Kormányrendelet 5/A. § (3) bekezdés c) pont ca) alpontja

9.3.6. Az intézmény a hozzáférések kezelése során a tervezett és megvalósult összerendeléseket és az ezeken keresztül megvalósított hozzáféréseket folyamatosan nyomon követi, gondoskodik azok összhangjának rendszeres ellenőrzéséről.

9.3.7. Az intézmény a hozzáférési rendben rendszerenként meghatározza legalább az alábbiakat:

- a) rendszerazonosító (hálózati név), hálózati kapcsolatok, adatkapcsolatok, portok és protokollok, a felhasználói hitelesítés módja,
- b) a rendszerszintű biztonsági beállítások,
- c) a helyi és távoli felhasználók, felhasználócsoportok, beépített felhasználói fiókok, fiók beállítások, helyi házirend tartalma – biztonsági házirend (például jelszóházirend, biztonsági naplózás stb.) – tartalma,
- d) címtár rendszerek esetében a felhasználók, felhasználócsoportok, beépített felhasználói fiókok, fiók beállítások, hozzáférés-vezérlési listák, szervezeti egységek, közzétett (megosztott) erőforrások, a címtár objektumokhoz tartozó hozzáférési jogok, a tartományok biztonsági beállításai (például jelszószabályok, naplózási beállítások),
- e) erőforrások hozzáférési engedélyei, hozzáférés-vezérlő listák, erőforrások eseménynaplózási beállítása,
- f) mappák megosztása, a megosztás paraméterei, a megosztáshoz és a fájlokhoz tartozó jogok,
- g) alkalmazási rendszerekben a felhasználók rendszeren belüli kezelésének, továbbá a felhasználói csoportok (szerepkörök) és az üzleti műveletek egymáshoz rendelésének, valamint az általános biztonsági beállítások (például jelszószabályok, naplózási beállítások, az adatkapcsolatok számára létrehozott technikai jellegű felhasználók) kezelésének eljárása,
- h) adatbázis kezelők esetében továbbá a fiók beállítások, a nem beépített szerepkörök rendszer- és objektum privilégiumai, profilok és biztonsági beállítások (például jelszószabályok, naplózási beállítások),
- i) a kiemelt jogosultságú rendszer fiókok (például rendszeradminisztrátori fiókok), valamint a technikai jellegű felhasználók és a felelősök nyilvántartása, a kezelésükre vonatkozó szabályok,
- j) azoknak a felhasználói fiókoknak a listája, amelyek esetén az intézmény szükségesnek tartja a vészhelyzeti elérhetőség biztosítását.

9.3.8. Az intézmény a rendszerek biztonsági beállításait a rendszerre vonatkozó szakmai „hardening” ajánlások, illetve a szállítótól kapott üzemeltetési kézikönyvek aktuális verziói alapján időszakosan felülvizsgálja és aktualizálja.

9.4. Felhasználói adminisztráció

9.4.1. Vonatkozó jogszabályi rendelkezés: *az intézménynél az élesüzemi rendszerben felállított végfelhasználói hozzáférések egységes, zárt rendszert alkotnak, melyek biztosítják az üzleti folyamatok megvalósulását, továbbá a végfelhasználók tevékenysége naplózásra kerül és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak;⁴⁹ az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek, továbbá a kiemelt jogosultságokkal elvégzett tevékenység naplózása*

⁴⁹ Kormányrendelet 5/B. § f) pontja

megvalósul, a napló fájlok sérthetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak;⁵⁰ az élesüzemi rendszerhez történő távoli hozzáférés szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött⁵¹. Az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események).⁵²

- 9.4.2. Az intézmény az informatikai rendszeréhez való hozzáférést egyedi, természetes személyekkel egyértelműen összerendelhető felhasználói fiókok használatához köti, a használatot az informatikai biztonsági szabályozási rendszerében szabályozza.
- 9.4.3. Az intézménynél a felhasználói fiókok létrehozása, törlése (tiltása), illetve módosítása a hozzáférési rendben meghatározottak szerint – jóváhagyott és dokumentált módon történik,
- 9.4.4. Az intézmény a felhasználói fiókok létrehozása és kiadása során biztosítja, hogy csak az a személy vehesse birtokba az azonosítót, akinek a részére azt létrehozták, és – az informatikai rendszeren belüli vagy önálló nyilvántartás vezetésével – biztosítja a felhasználói fiókok és a fiókok használatáért felelős felhasználók egyértelmű egymáshoz rendelését.
- 9.4.5. Az intézmény gondoskodik arról, hogy az informatikai rendszerekben mindenkor csak az aktuálisan engedélyezett felhasználók rendelkeznek jogosultsággal, és hogy ennek ellenőrzése azonnal elvégezhető legyen.
- 9.4.6. Az intézmény a jelszó komplexitási és lejáratási szabályokat az egyes rendszerekben a felhasználói fiókok használatával végezhető tevékenységek kockázataival arányosan, a felhasználók által kezelhető módon határozza meg.
- 9.4.7. Az ügyfeladatot és pénzügyi ágazati titkot tartalmazó rendszerekben alkalmazott azonosítók és jelszavak, eljárások és eszközök megválasztása során az intézmény figyelembe veszi a védendő érték, a lehetséges kockázatok és a szükséges ráfordítások körülményeit.
- 9.4.8. Az intézmény a felhasználói fiók be- és kilépés, jelszótároltatás és egyéb autentikációhoz kapcsolódó események adatait naplózza, azzal, hogy a jelszó sem a kritikus, sem más rendszerekben nem kerülhet naplózásra.
- 9.4.9. Távoli hozzáférések esetében az intézmény a felhasználói fiók mellett legalább még egy további, a felhasználót hitelesítő faktort – például dinamikus kódot, tanúsítványt – is használ.
- 9.4.10. Az intézmény a vészhelyzeti elérés módját a felhasználói fiókok kezelésének szabályai között rendezi, a vészhelyzetben elérhetővé tett felhasználói fiókokról egységes nyilvántartást vezet, és elvégzi a vészhelyzeti elérés megfelelésének időszakos ellenőrzését.
- 9.4.11. Az intézmény gondoskodik a technikai felhasználók jelszavaival kapcsolatos tárolási és felhasználási szabályok informatikai szabályzati rendszerben történő meghatározásáról, valamint azok kikényszerítéséről, figyelembe véve legalább a legkisebb jogosultság elvét és a „négysem” elvet.
- 9.4.12. Az intézmény a kockázataival arányos módon gondoskodik az informatikai rendszereiben a jelszóra vonatkozóan az alábbi szabályok bevezetéséről:

⁵⁰ Kormányrendelet 5/B. § g) pontja

⁵¹ Kormányrendelet 5/B. § h) pontja

⁵² Bszt.12. § (6) bekezdés c) pontja, Mpt. 77/A. § (5) bekezdés c) pontja, Öpt. 40/C. § (5) bekezdés c) pontja, Kormányrendelet 3. § (2) bekezdés c) pontja

- a) a jelszó minél több (min. 12, adminisztrátori vagy technikai szerepkörben min. 15.) karaktert vagy jelmondatot tartalmazzon,
- b) a jelszó ne legyen szótár alapú,
- c) a jelszó ne legyen könnyen kitalálható (ne utaljon a felhasználóra, rokonára, tulajdonára stb.),
- d) a legutoljára használt 5 jelszó ne legyen beállítható,
- e) a jelszó lejárata legalább 1 nap és legfeljebb 90 nap,
- f) legfeljebb 5 egymást követő sikertelen belépés esetén a fiók zárolásra kerül,
- g) az egymást követő sikertelen belépések közötti időtartamok (time-out period) növekednek,
- h) a rendszergazdák, alkalmazásgazdák és más, több szerepkörben is a rendszerhez férő felhasználók belépési azonosítói (például felhasználói és adminisztrátori) szerepkörök szerint kerüljenek szétválasztásra,
- i) a jelszavak tárolása – a technikai jelszavak megfelelően kontrollált, vészhelyzetre történő kezelésén kívül – minden esetben rejtjelezetten történjen,
- j) a kezdeti jelszó megváltoztatását az informatikai rendszer kényszerítse ki.

9.5. Hozzáférési és felhasználói adminisztrációs szabályok ellenőrzése

9.5.1. Az intézmény az informatikai biztonsági szabályozási rendszerben meghatározott eljárásrend szerint, az abban meghatározott időközönként, de legkésőbb évente a felhasználói azonosítók és a hozzájuk kapcsolódó jogosultságok dokumentált ellenőrzésével meggyőződik a hozzáférési és felhasználói adminisztrációs szabályok betartásáról.

9.6. Titkosítás, kulcskezelés, tanúsítványmenedzsment

9.6.1. Az intézmény az informatikai biztonsági szabályozási rendszerében rendelkezik az alkalmazott titkosítások, a kapcsolódó kulcskezelés és a tanúsítványmenedzsment szabályairól és eljárásairól.

9.6.2. Az intézmény az informatikai rendszereiben kizárólag nyílt, szabványos kriptográfiai eljárásokat és algoritmusokat alkalmaz.

9.6.3. Az intézmény a kriptográfiai kulcsok hosszúságát a kulcsok élettartama és a használt algoritmus (például szimmetrikus) sajátosságai szerint határozza meg.

9.6.4. Az intézmény folyamatosan figyelemmel kíséri az aktuális technológiai megoldásokat, és a kulcsok visszafejthetőségének egyszerűsödését. Az elavult megoldásokat cseréli, figyelembe véve a már korábban védett információk biztonságát is.

9.6.5. Az intézmény dokumentált, teljes körű, szabványos kriptográfiai kulcskezelési eljárással rendelkezik, ami kitér legalább az alábbiakra:

- a) biztonságos kulcselőállítás és kulcselosztás,
- b) biztonságos kulcstárolás, az autentikációs és a titkosítási kulcsok kezelése, tárolása,
- c) meghatározott időnkénti kulcscsere, lejárt élettartamú vagy kompromittálódott kulcsok visszavonása, lecserélése, megsemmisítése,
- d) kulcs megosztás és kettős hozzáférés alkalmazása és módszere,
- e) a titkosított állományok és a kapcsolódó kulcsok archiválása, a technikai fejlődés figyelembevételével.

- 9.6.6. Az intézmény gondoskodik arról, hogy a titkos kulcsok exportálása ne, kivételes esetben pedig csak rejtjelezett formában, a megfelelő kontrollok mellett, egyedileg történjen meg.
- 9.6.7. Az intézmény központi nyilvántartást vezet a saját maga által kiadott, valamint a külső szolgáltatótól vásárolt tanúsítványokról és a tanúsítványtároló eszközökről. A nyilvántartás aktualizálásáról folyamatosan gondoskodik.
- 9.6.8. Az intézmény a külső szolgáltatótól vásárolt tanúsítványok esetében meghatározza és biztosítja a tanúsítványkiadónál kapcsolattartóként megadott személyek helyettesítését.
- 9.6.9. Az intézmény gondoskodik a publikus kulcsú infrastruktúra (Public Key Infrastructure – PKI) rendszereinek megerősítéséről, információbiztonsági felülvizsgálatáról, és az architektúrális kialakítása során biztosítja a Certificate Authority (CA) szerverek és kulcsaik megfelelő védelmét, valamint gondoskodik a virtualizált megoldások megfelelő szétválasztásáról.
- 9.6.10. Az intézmény gondoskodik a PKI rendszer kiszolgálóinak és kulcsainak kompromittálódás ellen védett mentéséről.
- 9.6.11. Az intézmény gondoskodik arról, hogy az elvárható legjobb gyakorlat alapján kerüljenek beállításra a használatában lévő a CA kiszolgálók és az általuk kiadott tanúsítványok által használt algoritmusok, kulcshosszok, tanúsítvány template-k, használati funkciók, lejáratási idők, tanúsítvány tárolási és megosztási módok, visszavonási listák publikálása és érvényessége.
- 9.6.12. Az intézmény gondoskodik a PKI rendszerének folyamatos monitorozásáról, illetve az események - lehetőség szerinti automatikus - észleléséről és kezeléséről.
- 9.6.13. Az intézmény a kockázatokkal arányosan biztosítja a PKI rendszerei hibatűrését, rendelkezésre állását, a konfigurációjának és a kulcsainak mentését, a lényeges eseményeinek naplózását és központi naplógyűjtését és -kiértékelését, és folyamatosan gondoskodik a PKI környezeteihez kiadott – funkcionális és biztonsági – gyártói frissítések rendszeres telepítéséről.

10. MENTÉSI, ARCHIVÁLÁSI RENDSZER, HELYREÁLLÍTÁS, ADATHORDOZÓK KEZELÉSE

10.1. Vonatkozó jogszabályi rendelkezés:

Az intézménynek rendelkeznie kell az informatikai rendszer szoftver elemeire vonatkozó olyan biztonsági mentésekkel és mentési renddel, továbbá helyreállítási tervvel, amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik, továbbá a mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolnia, és gondoskodnia kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.⁵³ Az élesüzemi rendszer adatmentési és visszaállítási rendje biztosítja a rendszer biztonságos visszaállítását, továbbá a mentés-visszaállítás a vonatkozó szabályzat szerinti gyakorisággal és dokumentáltan tesztelt⁵⁴. Az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell az adathordozók szabályozott és biztonságos kezeléséről.⁵⁵ Az intézménynél az élesüzemi rendszer adathordozóinak védelme

⁵³ Bsz. 12. § (7) bekezdés e) pontja és (8) bekezdése, Mpt. 77/A. § (6) bekezdés e) pontja, Öpt. 40/C. § (6) bekezdés e) pontja, Kormányrendelet 3. § (3) bekezdés e) pontja, és (4) bekezdése

⁵⁴ Kormányrendelet 5/B. § d) pontja

⁵⁵ Bsz. 12. § (6) bekezdés f) pontja, az Mpt. 77/A. § (5) bekezdés f) pontja, az Öpt. 40/C. § (5) bekezdés f) pontja, Kormányrendelet 3. § (2) bekezdés f) pontja,

*szabályozott, megfelelően korlátozott, és a korlátozásokat rendszeres felülvizsgálatokkal és ellenőrzésekkel is fenntartják.*⁵⁶

10.2. Általános elvárások:

Az adatok mentésének célja, hogy az adatok a kritikus helyreállítási időn (Recovery Time Objective, a továbbiakban: RTO) belül a kritikus visszaállítási pontra (Recovery Point Objective, a továbbiakban: RPO), illetve adott pontra történő helyreállítással lehetővé tegye az adatok elérhetőségét a megfelelő hozzáférési jogosultságok biztosításával. Az MNB elvárja, hogy az intézmény az archiválások során biztosítsa, hogy az adatok egy későbbi időpontban is visszaállíthatók legyenek, ezért szükséges gondoskodnia az erre alkalmas technológiák és megoldások alkalmazásáról.

10.3. A mentés és archiválás szabályai

10.3.1. Az intézmény az informatikai biztonsági szabályozási rendszerében meghatározza az adatok biztonsági mentésével, archiválásával, valamint azok helyreállításával és ellenőrzésével kapcsolatos szabályokat és eljárásrendeket.

10.3.2. Az intézmény a mentési rendjét – a szolgáltatásfolytonossági követelményekkel összhangban - az elfogadott RTO és RPO (lásd 10.2 pont) figyelembevételével úgy alakítja ki, hogy a mentések típusa, gyakorisága és példányszáma elfogadható idő- és adatvesztési kockázatot eredményezzen.

10.3.3. Az intézmény gondoskodik arról, hogy:

- a) a mentett adatok nyilvántartásba vétele megtörténjen;
- b) az adatok mentése, illetve archiválása mellett az adatok visszaállításához szükséges valamennyi egyéb adat és szoftver komponens is visszaállíthatóan mentésre, illetve archiválásra kerüljön, vagy mentésük, illetve archivált állományuk létezzen;
- c) a mentésre, illetve archiválásra alkalmazott adathordozó megválasztása az adathordozó felhasználhatóságának gyártói korlátozásai – például adatmegőrzési idő, újraírhatóság száma, tárolási előírások – figyelembevételével történjen;
- d) a mentéseket és archív adatokat tartalmazó adathordozók kezelése a rajtuk tárolt adatok biztonsági osztályához rendelt előírások szerint történjen;
- e) a mentéseket és archív adatokat tartalmazó adathordozók a forrásrendszerrel azonos szintű biztonságos fizikai és logikai hozzáférés védelem mellett kerüljenek megőrzésre;
- f) a mentett és az archív állományok adatait tartalmazó adathordozók, valamint az azok visszatöltéséhez szükséges berendezések mindenkor – a tartalék helyszínen is (lásd 11.2.7. pont) – rendelkezésre álljanak;
- g) a titkosított mentésben vagy archív állományokban lévő adatok a technológia változása esetén is a megfelelő védelemben részesüljenek.

10.3.4. Az intézmény a mentések tűzbiztos védelmét úgy biztosítja, hogy a helyreállításra szolgáló mentéseket és archív állományokat több helyszínen – egyrészt az éles környezettől elkülönítetten, a tartalék helyszínen, másrészt az éles adatoktól elkülönült, zárható és legalább 30 perces tűzállóságú önálló helyiségben, az épület egy másik tűzszakaszában vagy az éles adatokat tartalmazó épülettől a tűzvédelmi szabályoknak megfelelő módon elválasztott másik épületben – tárolja.

⁵⁸ Kormányrendelet 5/B. § n) pontja

10.3.5. Az intézmény a mentési rendjében rendelkezik legalább az alábbi operatív utasítások elkészítéséről:

- a) a pénzügyi szervezet mentési rendszerének összefoglaló leírása, amely tartalmazza:
 - aa) a mentett adatok körének teljes körű meghatározását,
 - ab) a mentések módját, az alkalmazott mentési szoftverek és a mentőeszközök megnevezését, a mentett állományok őrzési helyét,
 - ac) az egyes mentésekhez tartozó lehetséges adatvesztési eseteket (például az előző napi mentésből a tárgynap napközbeni tranzakciói nem állíthatók vissza),
 - ad) a mentések készítésének (futtatásának) időintervallumát,
 - ae) a mentett állományok megőrzési idejét,
 - af) a mentett állományok nyilvántartásának módját,
 - ag) az elkészített mentések olvashatóságának az ellenőrzésére alkalmazott eljárásokat, az ellenőrzés gyakoriságát;
- b) mentési eljárások, amelyek a mentések elvégzésére és annak ellenőrzésére vonatkozó eljárások;
- c) visszatöltési eljárások, amelyek az egyes mentések visszatöltésére és a visszatöltés megfelelőségének az ellenőrzésére vonatkozó eljárások;
- d) helyreállítási eljárások, amelyek a mentéssel érintett informatikai, illetve adatkommunikációs rendszerek visszatöltés utáni visszaállítására és a visszaállítás megfelelőségének az ellenőrzésére vonatkozó eljárások.

10.3.6. Az intézmény a mentési rendjében meghatározottak szerint rendszeresen gondoskodik a mentések meglétének és az adatok visszaállíthatóságának dokumentált ellenőrzéséről.

10.4. Archiválás

10.4.1. Vonatkozó jogszabályi rendelkezés: *a pénzügyi intézménynek rendelkeznie kell jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizték.*⁵⁷

10.4.2. Az intézmény a jogszabályban meghatározott nyilvántartásairól a dokumentált mentési rend alapján archivált mentéseket készít, és azokat az ágazati, vagy vonatkozó jogszabályokban meghatározott ideig – vonatkozó szabályozás hiányában legalább öt évig – bármikor visszakereshetően, helyreállíthatóan megőrzi (archív állományok).

10.4.3. Az intézmény az adattároló berendezéseinek, rendszereinek a cseréje során gondoskodik arról, hogy az archív adatok az újonnan üzembe állított rendszerekbe átkerüljenek, vagy gondoskodik a régi rendszerek üzemben tartásáról, illetve arról, hogy azok – az adatok visszaállíthatósága érdekében – mindenkor üzembe állíthatók legyenek.

10.5. Adathordozók kezelése

10.5.1. Adathordozó minden olyan eszköz vagy szerelem, amely alkalmas az adatok tárolására.

10.5.2. Az intézmény az informatikai biztonsági szabályozási rendszerében rendelkezik az adathordozók biztonságos kezeléséről, beleértve a tiszta asztal – tiszta képernyő elveket.

⁵⁷ Bszt. 12.§ (7) bekezdés f) pontja, Mpt. 77/A. § (6) bekezdés f) pontja, Öpt. 40/C. § (6) bekezdés f) pontja, Kormányrendelet 3. § (3) bekezdés f) pontja

10.5.3. Az intézmény az adathordozók kezelése során betartja és betartatja az adathordozón tárolt adatok biztonsági osztályára előírt védelmi előírásokat (beleértve a fizikai és logikai hozzáférési szabályokat is).

10.5.4. Az adathordozó üzemből kivonása esetén az ügyfeladatot, valamint a pénzügyi ágazati titok körébe tartozó adatokat az adathordozókon visszaállíthatatlan módon törli, az adathordozót megsemmisíti.

10.5.5. Az intézmény az adathordozókról egyedi nyilvántartást vezet, amely tartalmazza legalább

- a) az adathordozók típusát;
- b) egyedi azonosítóját;
- c) az adathordozóhoz rendelt felelős személyt;
- d) adathordozó helyét.

10.5.6. Az intézmény a kockázataival arányosan gondoskodik az adathordozókon tárolt adatok titkosításáról, valamint a titkosítási kulcsok 9.6. pontban meghatározott kezeléséről.

10.6. Mentéssel és archiválással kapcsolatos adatkezelés

10.6.1. Az intézmény a mentések és archiválások során biztosítja, hogy az adatok a célhoz kötöttség elve szerint az adatvédelmi és az ágazati jogszabályok előírásai szerint kerüljenek tárolásra. AZ MNB elvárja, hogy a mentések kialakítása során az intézmény biztosítsa, hogy az ügyfeladatok és a pénzügyi ágazati titok körébe tartozó adatok a csak a jogszabályi előírások szerinti időtartamában kerüljenek tárolásra. Ezt követően szükséges az adatok törlésének, vagy az adatok ügyféllel történő összekapcsolásának visszaállíthatatlan megszüntetése úgy, hogy az ügyfeladat és a pénzügyi ágazati titok körébe tartozó adat az érintettel a továbbiakban ne legyen összefüggésbe hozható, a kapcsolat közöttük ne legyen helyreállítható.

10.6.2. A mentések és archív állományok tárolása és kezelése során szükséges biztosítani az adathordozókra vonatkozó szabályok (lásd. 10.5. pont) érvényesülését.

11. SZOLGÁLTATÁSFOLYTONOSSÁG

11.1. Vonatkozó jogszabályi rendelkezés: *az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel (a továbbiakban: szolgáltatásfolytonossági terv).*⁵⁸ Továbbá az intézménynek rendelkeznie kell a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb – a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal.⁵⁹ A katasztrófa-helyreállítási terv rendszeresen tesztelt.⁶⁰

11.2. A szolgáltatásfolytonosságot akadályozó rendkívüli események kezelésére szolgáló terv

11.2.1. Az MNB elvárja, hogy a szolgáltatásfolytonossági terv biztosítsa az üzletszabályzatban és az aktuális hirdetményekben közzétett működési feltételeket.

⁵⁸ Bszt. 12. § (7) bekezdés g) pontja, Mpt. 77/A. § (6) bekezdés g) pontja, Öpt. 40/C. § (6) bekezdés g) pontja, Kormányrendelet 3. § (3) bekezdés g) pontja

⁵⁹ Bszt. 12. § (7) bekezdés c) pontja, Mpt. 77/A. § (6) bekezdés c) pontja, Öpt. 40/C. § (6) bekezdés c) pontja, Kormányrendelet 3. § (3) bekezdés c) pontja

⁶⁰ Kormányrendelet 5/B. § k) pontja

11.2.2. Az intézmény az informatikai biztonsági szabályozási rendjébe illesztve elkészíti a szolgáltatásfolytonossági tervét, amelyben meghatározza a szolgáltatás folytonosságának biztosításához szükséges szabályokat, eljárásrendeket és operatív utasításokat, valamint ezek ellenőrzésének szabályait.

11.2.3. A szolgáltatásfolytonossági terv elkészítése során az intézmény meghatározza kritikus üzleti szolgáltatásait, azonosítja a szolgáltatások nyújtásához szükséges folyamatait, meghatározza a folyamatok lehetséges kiesései eseteit, meghatározza az üzleti igények és az adatbesorolás alapján elfogadott RPO-kat és RTO-kat (lásd 10.2 pont), és ennek során kitér legalább az alábbi típusok életszerű eseteire:

- a) természeti csapások, ember okozta működési rendellenességek, informatikai és adatkommunikációs infrastruktúra hibákból fakadó, a munkahely használatát akadályozó tényezők okozta részleges, teljes szolgáltatás kiesés különböző esetei,
- b) az alkalmazott üzemeltetési rendszer, illetve az informatikai üzemeltetési helyszín használhatatlanná válása,
- c) külső szolgáltatások hibás teljesítése, teljes kiesése vagy elérhetetlenné válása,
- d) a kockázatelemzés során feltárt, az intézményre jellemző kritikus esetek.

11.2.4. Az intézmény kidolgozza, és szolgáltatásfolytonossági tervében dokumentálja:

- a) az informatikai rendszer kiesése idején követendő üzleti helyettesítő eljárásokat,
- b) az informatikai és adatkommunikációs tartalék rendszerekre való átállás, valamint a helyreállításra vonatkozó részletes, operatív eljárásokat,
- c) a normál üzemre történő visszaállás operatív eljárásait,
- d) az egyes eljárásokra vonatkozóan az eljárások végrehajtóit, illetve a végrehajtás felelőseit,
- e) az egyes kiesési esetekre vonatkozóan a belső felelősségi rendet és a külső kommunikáció rendjét.

11.2.5. A szolgáltatásfolytonossági eljárások ellenőrzése és bevezetése keretében az intézmény

- a) valós eljárások során, dokumentált teszteléssel meggyőződik az eljárások alkalmazhatóságáról;
- b) a szolgáltatásfolytonossági eljárásainak tesztelése során a sikeres záró teszt lényeges körülményeit – ideértve a teszt eljárások egyes lépéseit, a végrehajtás tervezett és mért időtartamát is –, az elvégzett tevékenységeket és az egyéb megállapításokat együttesen dokumentálja;
- c) minden érintett számára dokumentáltan oktatja az eljárásokat, feladatokat és felelősségeket, valamint felkészíti a szervezetét az eljárások alkalmazására;
- d) dokumentáltan – az üzleti terület bevonásával – meggyőződik arról, hogy az üzleti elvárások alapján meghatározott RTO-k tarthatók-e, valamint az RPO-ra (lásd 10.2 pont) történő visszaállás lehetséges-e;
- e) amennyiben a d) pontban foglaltak nem teljesülnek, akciótervet dolgoz ki a teljesülés érdekében;
- f) a szolgáltatásfolytonossági tesztelés eredményét dokumentálja, azt a vezetőség dokumentáltan jóváhagyja;

- g) az üzleti vagy szolgáltatási eljárásokban, informatikai folyamatokban, technológiai vagy releváns jogszabályi környezetben történt minden változás esetén, vagy bekövetkezett incidenst követően, de legkésőbb a kockázatelemzés felülvizsgálata során a szolgáltatásfolytonossági tervet felülvizsgálja, valamint dokumentáltan teszti és jóváhagyja;
- h) a szolgáltatásfolytonossági tervét a székhelyétől, illetve fő telephelyétől eltérő helyszínen, illetve a helyreállításhoz szükséges helyszíneken is, aktuális állapotban, biztonságosan tárolja.

11.2.6. Az intézmény rendelkezik a szolgáltatások folytonosságát biztosító tartalékberendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb megoldásokkal. Ennek érdekében az intézmény

- a) szolgáltatásai folytonosságát biztosító tartalékberendezések alkalmasak az élesüzemi berendezések meghibásodásakor automatikusan vagy manuális közreműködéssel RTO időn belül RPO szerinti szolgáltatási pontról (lásd 10.2 pont) biztosítani legalább a kritikus folyamatok teljes körű működését;
- b) az a) pontban meghatározott tartalék berendezéseket az élesüzemi rendszereket tartalmazó telephelytől biztonsági kockázatok figyelembe vételével elkülönített helyszínen (vö. a 11.2.7. ponttal) tárolja;
- c) rendelkezik olyan tartalék feldolgozási helyszínnel, amelyben a szolgáltatások folytonosságának biztosítása érdekében rendelkezésre állnak a kritikus üzleti terület munkatársai foglalkoztatására alkalmas berendezések;
- d) a tartalékberendezéseket tartalmazó, valamint a tartalék feldolgozási helyszínt a 11.2.7. pontban meghatározott kritériumok alapján választja ki.
- e) amennyiben nem rendelkezik az a)-d) pontban meghatározottakkal, úgy azokra – az ott meghatározottakkal egyenértékű – helyettesítő megoldásokat alkalmaz (például az eszközök és a telephelyek rendelkezésre bocsátására szerződést köt).

11.2.7. Tartalék helyszín: Az intézmény a székhelye, fő telephelye, illetve az élesüzemi rendszereit tartalmazó helyszíne elérhetetlensége esetére a szolgáltatásfolytonosság biztosítása érdekében az alábbi szempontok alapján választ tartalék üzemi, illetve tartalék feldolgozási helyszínt (a továbbiakban együtt: tartalék helyszín):

- a) a tartalék helyszín az élesüzemi rendszereit tartalmazó helyszínhez képest olyan földrajzi távolságra található, hogy katasztrófaesemények (például tüzeset, földrengés, árvíz, tűzserzészeti események) vagy közlekedési események, valamint egyéb – az adott helyszín használatát vagy az oda történő bejutást akadályozó – események a fő- és tartalék helyszínt egyidejűleg ne érintsék;
- b) az a) pontban foglaltak érdekében a két helyszín egymástól légvonalban mért távolsága a korábban kialakított székhely, illetve telephelyek esetén nem lehet kevesebb, mint 400 méter; új kialakítás esetén haladja meg az 1000 métert;
- c) a helyszínek egymástól független áramellátási, távközlési és adatkommunikációs szolgáltatási betáplálással rendelkezzenek;
- d) a tartalék helyszín megközelítése és az átállás teljes időtartama egybeszámítva nem haladja meg az RTO-t (lásd 10.2 pont).

11.2.8. Előremutató gyakorlat

A szolgáltatásfolytonossági tervezés során az alábbiak figyelembevételre javasolt:

- a) az intézmény szolgáltatásfolytonossági terve olyan forgatókönyvszerű operatív intézkedési terv, amely lehetővé teszi az eljárások gyors, hibamentes végrehajtását;
- b) a szolgáltatásfolytonossági tervet – amennyiben azt az intézmény célszerűnek tartja – több dokumentumban készíti el (például az üzletmenet folytonossági terv az üzleti helyettesítő eljárásokat, az informatikai katasztrófa helyzet elhárítási terv az informatikai rendszer működésének a helyreállítását rögzíti);
- c) amennyiben az intézmény elektronikusan támogatott szolgáltatásfolytonossági rendszert (BCM) használ, gondoskodik arról, hogy a rendszer elérhetetlenné válásakor is képes legyen biztosítani a rendszerben tárolt aktuális információkat a tartalék helyszínen is.

12. SZEMÉLYI BIZTONSÁG

12.1. Vonatkozó jogszabályi rendelkezés: *az élesüzemi rendszer üzemeltetésében és használatában részt vevő személyek rendszeres biztonságtudatosági oktatáson vesznek részt, valamint az intézmény dolgozóinak munkaügyi szabályozása megfelel a biztonsági előírásoknak.*⁶¹

12.2. Biztonságtudatosági oktatás

12.2.1. Az intézmény az informatikai biztonsági szabályozási rendszerében meghatározza az informatikai biztonságtudatosági oktatás szabályait, eljárásrendjét.

12.2.2. Az intézmény gondoskodik az üzleti folyamatai támogatására szolgáló élesüzemi informatikai rendszerekhez és az azokban tárolt adatokhoz hozzáférő felhasználók rendszeres, az új belépők esetén a belépéstől számított 3. hónapig bezárólag, a többi felhasználó esetében legkésőbb éves szinten történő dokumentált biztonságtudatosági oktatásáról.

12.2.3. Az intézmény folyamatosan gondoskodik az élesüzemi rendszerek üzemeltetésében részt vevő személyek megfelelő szakmai színvonalon történő biztonságtudatosági képzéséről.

12.2.4. Az intézmény a képzésekhez éves képzési tervet készít, a külső képzéseken történő részvételét a költségvetése tervezésekor figyelembe veszi.

12.2.5. Előremutató gyakorlat

Az intézmény az üzemeltetők és fejlesztők biztonsági oktatásának tervezésekor figyelembe veheti az üzemeltetők és fejlesztők speciális részterületeire, valamint a tervezés során esetlegesen bevezetésre kerülő új rendszerekre vonatkozó biztonsági képzéseket annak érdekében, hogy releváns információk birtokába kerüljenek.

12.3. A személyi biztonság munkaügyi szabályozása

12.3.1. Az intézmény azon munkaköröket, amelyek ellátása során a munkavállalók az intézmény üzleti folyamataihoz közvetlenül vagy közvetve hozzáférnek – beleértve a külső vagy harmadik személyek hozzáféréseit is – az adatbesorolás alapján biztonsági osztályba sorolja. Az intézmény informatikai biztonsági szabályozási rendszerében rögzíti a munkakörökhöz rendelt biztonsági osztályokat és az azokhoz tartozó biztonsági kritériumokat.

⁶¹ Kormányrendelet 5/B. § s) pontja

12.3.2. Az intézmény adott munkakörbe történő munkaerő felvételkor ellenőrzi, hogy az érintett munkavállaló az adott munkakörhöz tartozó biztonsági osztálynak megfelelő biztonsági kritériumokat teljesíti-e.

12.3.3. Az intézmény belső szabályozási rendszerében szabályozza a munkakörök és a munkavállalók szerepének (adathozzáféréseinek) változásával kapcsolatos biztonsági eljárásrendet.

V. ELLENŐRZÉS

13. FÜGGETLEN ELLENŐRZÉS

13.1. Az ellenőrzés szabályai, a biztonsági rendszer ellenőrzése

13.1.1. Vonatkozó jogszabályi rendelkezés: *az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével az intézménynek meg kell határoznia a folyamatba épített ellenőrzési követelményeket és szabályokat.⁶² Az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljes körűségét biztosító ellenőrzésekről, eljárásokról⁶³; az élesüzemi rendszer üzemeltetési folyamatai szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek⁶⁴; az élesüzemi rendszerhez való végfelhasználói hozzáférés mind alkalmazási, mind pedig infrastruktúra szinten szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött⁶⁵; az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek⁶⁶; az élesüzemi rendszerhez történő távoli hozzáférés szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött⁶⁷; az élesüzemi rendszer adatkommunikációs és rendszerkapcsolatai dokumentáltak és ellenőrzöttek annak érdekében, hogy az adatkommunikáció bizalmassága, sérthetetlensége és hitelessége biztosítható legyen⁶⁸; az élesüzemi rendszer adathordozóinak védelme szabályozott, megfelelően korlátozott, és a korlátozásokat rendszeres felülvizsgálatokkal és ellenőrzésekkel is fenntartják⁶⁹.*

13.1.2. Az intézmény az informatikai biztonsági szabályozási rendszerében rendelkezik az informatikai biztonság független, rendszeres, teljes körű ellenőrzéséről. Függetlenség alatt az értendő, hogy az ellenőrzési terület nem vonható be az ellenőrzendő kontrollintézkedések megtervezésébe, kiválasztásába, implementálásába vagy azok működtetésébe, és nincs alárendelt viszonyban az ellenőrzött területtel.

⁶² Bszt. 12. § (4) bekezdése, Mpt. 77/A. § (3) bekezdése, Öpt. 40/C. § (3) bekezdése, Kormányrendelet 2. § (3) bekezdése

⁶³ Bszt. 12. § (6) bekezdés b) pontja, Mpt. 77/A. § (5) bekezdés b) pontja, Öpt. 40/C. § (5) bekezdés b) pontja, Kormányrendelet 3. § (2) bekezdés b) pontja

⁶⁴ Kormányrendelet 5/B. § b) pontja

⁶⁵ Kormányrendelet 5/B. § e) pontja

⁶⁶ Kormányrendelet 5/B. § g) pontja

⁶⁷ Kormányrendelet 5/B. § h) pontja

⁶⁸ Kormányrendelet 5/B. § j) pontja

⁶⁹ Kormányrendelet 5/B. § n) pontja

13.1.3. Az intézmény gondoskodik az informatikai biztonság – szabályzatban meghatározott – független és rendszeres ellenőrzéséről, oly módon, hogy minden részterület legkésőbb 3 évente ellenőrzésre kerüljön.

13.1.4. Az intézmény az informatikai biztonság rendszeres ellenőrzése során gondoskodik legalább az alábbi ellenőrzések elvégzéséről:

- a) az üzemeltetési folyamatok szabályzatban foglaltaknak megfelelően működnek és dokumentáltak;
- b) a felhasználói hozzáférések, jogosultságok megfelelően szabályozottak és dokumentáltak, a rendszerekben beállított hozzáférések megfelelnek a hozzáférési jogosultsági engedélyekben foglaltaknak, valamint az összeférhetetlenségi szabályoknak;
- c) a távoli hozzáférések a szabályzásban foglaltak szerint, a dokumentálásnak (engedélyezésnek) megfelelően kerültek beállításra;
- d) az adatkommunikációs és rendszerkapcsolatok a dokumentációknak megfelelően kerültek kialakításra, a változások megfelelően dokumentáltak, engedélyezettek, a dokumentációk és a beállítások alkalmasak az adatkommunikáció bizalmosságának, sértetlenségének és hitelességének biztosítására és ellenőrizhetőségére;
- e) a belső és elkülönített hálózati zónákban lévő rendszerekre vonatkozó sérülékenységvizsgálatok az intézmény belső szabályzati rendszerében meghatározott folyamat szerint legkésőbb évente, a bankkártya rendszerek, webes ügyfélkiszolgáló rendszerek, mobilalkalmazások és az azokat kiszolgáló rendszerek vonatkozásában legkésőbb negyedévente ismételve, valamint a kockázatként meghatározott kritikus hibák javítása haladéktalanul, a nem kritikus hibák javítása a kockázatokkal arányos ütemezés szerint megtörténik;
- f) az Internet felől elérhető alkalmazások penetrációs tesztje a kockázatként meghatározott hibák javítása után, az üzembe állítást megelőzően, illetve bármely a biztonságot érintő változtatás alkalmával, majd legkésőbb évente ismételve megtörténik;
- g) valamennyi rendszerkomponens esetében a beállítások időszakos felülvizsgálata, és a nem biztonságos, illetve szükségtelen szolgáltatások – például szkriptek, driverek, portok, szervizek – törlése, illetve tiltása megtörténik;
- h) a biztonsági javító csomagok az informatikai rendszer komponensekre és szoftverekre a kockázatoktól függően, valamint az előzetes teszt üzemét követően a gyártói javító csomagok telepítése megtörténik, vagy az intézmény gondoskodik kompenzáló intézkedésekről.

13.1.5. Előremutató gyakorlat

Az intézmény az ellenőrzéseket az elvártnál gyakrabban is végezheti, az informatikai biztonság folyamatos fenntartása érdekében a fentiekben túl más ellenőrzéseket is folytathat.

13.2. Informatikai ellenőrző rendszer

13.2.1. Vonatkozó jogszabályi rendelkezés: *az intézmény kiépíti az informatikai rendszere biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működteti.*⁷⁰

⁷⁰ Bszt. 12. § (5) bekezdése, Mpt. 77/A. § (4) bekezdése, Öpt. 40/C. § (4) bekezdése, Kormányrendelet 3. § (1) bekezdése

13.2.2. Az intézmény informatikai rendszerei automatikus ellenőrző rendszerét úgy alakítja ki, hogy az képes legyen biztosítani, hogy az informatikai rendszer hibáinak észlelése és azok megszüntetése a szolgáltatásfolytonossági tervben meghatározott rendelkezésre állási időknél megfelelően megtörténhessen. Ennek biztosítása érdekében az intézmény:

- a) felhasználói támogató szervezetet üzemeltet;
- b) olyan automatikus rendszerfelügyeleti és riasztó rendszert működtet, amely alkalmas legalább a 6.2.2, a 0. pontban foglaltak, valamint az informatikai incidensek azonnali riasztására;
- c) a riasztásokat úgy állítja be, hogy a munkaidőben és azon túl észlelt incidensek kezelése is az elvárt helyreállítási időn belül megtörténhessen.

14. NAPLÓZÁS

14.1. Vonatkozó jogszabályi rendelkezés:

az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is.⁷¹ A rendszer megfelelő műszaki és eljárásrendi megoldásokkal nyomon követi a védendő információk minden változtatását, melyek biztosítják, hogy még a jogosult általános és privilegizált felhasználók sem tudják törölni vagy módosítani a naplót vagy egyéb nyomon követést biztosító információkat.⁷² Az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események.⁷³ Az élesüzemi rendszerben a végfelhasználók tevékenysége naplózásra kerül és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak; az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságokkal elvégzett tevékenység naplózása megvalósul, a napló fájlok sérthetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak.⁷⁴

14.2. Általános elvárások:

Az intézmény a kritikus védendő információk változását dokumentálja (naplózza), a naplózás szabályait úgy határozza meg, hogy a nyomon követés és a naplók értelmezése azonnal elvégezhető legyen, és a szokásostól eltérő változások esetén riasztás történjen. Az intézmény biztosítja a napló állományok sérthetlenségét, folyamatosan gondoskodik a naplókiértékelésről, a naplózási szabályok betartását technológiai megoldásokkal is kikényszeríti.

14.3. Naplózás szabályozása:

⁷¹ Bszt. 12. § (6) bekezdés d) pontja, Mpt. 77/A. § (5) bekezdés d) pontja, Öpt. 40/C. § (5) bekezdés d) pontja, Kormányrendelet 3. § (2) bekezdés d) pontja

⁷² Kormányrendelet 5/A. § (3) bekezdés c) pont cb) alpontja

⁷³ Bszt. 12. § (6) bekezdés c) pontja, Mpt. 77/A. § (5) bekezdés c) pontja, Öpt. 40/C. § (5) bekezdés c) pontja, Kormányrendelet 3. § (2) bekezdés c) pontja

⁷⁴ Kormányrendelet 5/B. § f) pontja és g) pontja

14.3.1. Az intézmény az informatikai biztonsági szabályzati rendjében meghatározza a kritikus védendő információk nyomon követésének (naplózás) és ellenőrzésének (kiértékelésének) szabályozását. Ennek keretében az intézmény

- a) kritikus rendszerei – ideértve az adathálózati eszközöket, az informatikai biztonsági- és egyéb felügyeleti rendszereket is – naplózási beállításainak, paraméterezéseinek, rendszertípusonként a naplózott eseményeknek, a naplók legalább elégséges adattartalmának operatív utasításai elkészítését, dokumentálását és felülvizsgálatát az informatikai biztonsági szabályozási rendszerben szabályozza;
- b) üzemeltetési, informatikai biztonsági és üzleti területe együttesen meghatározza és dokumentálja azokat az informatikai biztonsági eseményeket, amelyeket észlelni szükséges, valamint meghatározza a detektálás és naplómegőrzés (tárterület, idő, mód), valamint a naplók sértetlensége alapját képező feltételeket;
- c) naplózási rendjében előírja az egyes naplóállományok ellenőrzésének módját, gyakoriságát, időpontját, felelősét, a beszámolás módját, valamint meghatározza a felügyelni kívánt eseményeket, az értesítendőkhöz közt, az azonnali riasztás eseteit és módját.

14.3.2. Az intézmény a naplózás szabályozási rendszerében kitér legalább

- a) az operációs rendszerek, informatikai hálózat, a szerverek, az alkalmazási rendszerek, adatbázisok, mappastruktúrák, informatikai és hálózati rendszerelemek hozzáférése,
- b) az alkalmazási rendszereiben történő, az ügyfél- és pénzügyi ágazati titok körébe tartozó adatok (beleértve a tranzakciós adatok) változásai,
- c) az információs és hálózati rendszerelemek beállításai, paraméterezései naplózására és naplókiértékelésére.

14.3.3. Az intézmény a naplózás szabályozási rendszerében meghatározottakat technológiai megoldásokkal is kikényszeríti, gondoskodik a naplóállományok sértetlenségéről.

14.4. Riasztás, azonnali reagálás:

Az intézmény a kritikus védendő információk nyomon követésének (naplózás) és ellenőrzésének (kiértékelésének) során biztosítja az azonnali riasztást igénylő eseményekre az azonnali reagálás feltételeit.

14.5. Előremutató gyakorlat

14.5.1. Az intézmény megfontolja, és kockázatai arányában dönt a naplóbejegyzések központi gyűjtéséről, valamint a bejegyzések központi operátori, illetve automatikus kiértékeléséről.

14.5.2. Az intézmény a központi automatikus kiértékelési rendszer bevezetése esetén – az üzembe állítást megelőzően – gondoskodik a teljes körű tesztelésről, és a sikeres tesztelést követően az éles üzem teljes körű bevezetéséig az operátori kiértékelést változatlan formában fenntartja.

15. KISZERVEZÉS ELLENŐRZÉSE

- 15.1.1. A kiszervezett tevékenység szerződésben foglaltaknak megfelelő ellátását az intézmény a kiszervezési szerződésben, valamint az ágazati törvényekben⁷⁵ meghatározott módon és rendszerességgel ellenőrzi. Az intézmény az ellenőrzések során – amennyiben annak hatálya alá tartozik – figyelembe veszi a külső szolgáltatók igénybevételéről szóló MNB ajánlásban foglaltakat.
- 15.1.2. Az intézmény és a kiszervezett tevékenységet végzők a kiszervezési tevékenységek végzésére vonatkozó szerződésükben vagy ahhoz kapcsolódóan rögzítik a kiszervezett tevékenység végzője által minimálisan elkészítendő szabályzatokat, és ezeket az intézmény – a kiszervezési szerződésben foglaltaknak megfelelő teljesítés ellenőrzése keretében – vizsgálja.
- 15.1.3. Az intézmény a kiszervezett tevékenységre vonatkozó kockázatelemzés megtörténtét – a kiszervezési szerződésben foglaltaknak megfelelő teljesítés ellenőrzése keretében – vizsgálja, a vizsgálat eredményét dokumentálja, és azt a vezetőség értékeli.
- 15.1.4. Az intézmény – a kiszervezési szerződésben foglaltaknak megfelelő teljesítés ellenőrzése keretében – meggyőződik arról, hogy a kiszervezett tevékenység szolgáltatásfolytonossági eljárásai megfelelőek-e, és biztosítják-e az intézmény szolgáltatásfolytonossági követelményeit.

16. AZ INFORMATIKAI RENDSZER FUNKCIONÁLIS ALKALMASSÁGÁNAK KÖVETELMÉNYE

16.1. Vonatkozó jogszabályi rendelkezés:

*a szoftvereknek együttesen alkalmasaknak kell lenniük a működéshez szükséges és jogszabályban előírt adatok nyilvántartására, a pénzeszközök és a pénzügyi eszközök biztonságos nyilvántartására, az intézmény tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra, ideértve a pénzforgalmi számlák cégbíró felé történő bejelentését is, a tárolt adatok ellenőrzéséhez való felhasználására, valamint a biztonsági kockázattal arányos logikai védelemre és a sérthetlenség védelmére.*⁷⁶

16.2. Általános elvárások:

- 16.2.1. Az intézmény alkalmazási rendszerei eleget tesznek a vonatkozó pénzügyi-számviteli jogszabályi előírásoknak, így különösen
- a pénzügyi tranzakciókat szigorúan naplózott módon, idősorosan vezeti (ahol az időrend – akár más tranzakciókkal is összevethető módon – pontosan igazolható), és lezárt tranzakciók utólagos módosítását nem, csak a sztornó tételek dokumentálása és a sztornózásra vonatkozó szabályozás (külön engedély, naplózás, nyilvántartás stb.) betartása mellett engedélyezi,
 - az üzleti és a biztonsággal kapcsolatos tranzakciókat egyaránt naplózza,
 - belső jogosultsági rendszere lehetővé teszi a pénzügyi műveleteknek szerepkörök szerinti megosztását, az összeférhetetlen szerepkörök elkülönítését, ideértve a biztonsági adminisztrációs és az üzleti műveletek elkülönítését is;

⁷⁵ Bszt. 81. § (1) bekezdése, Hpt. 68. § (6) és (10) bekezdése, Mpt. 77/B. § (5) és (9) bekezdése, Öpt. 40/D. § (5) és (9) bekezdése

⁷⁶Bszt.12.§ (10), bekezdése Mpt.77/A.§ (8) bekezdése , Öpt.40/C.§ (8) bekezdése, Kormányrendelet 4. § (2) bekezdése

d) a tárolt adatokat és a naplókat ellenőrzés esetén haladék nélkül, közvetlenül az informatikai rendszerből képes kinyerni.

16.2.2. Az intézmény az informatikai rendszerét időben felkészíti az országos rendszerek, valamint a jogszabályi előírások változására, az üzleti igények teljesítésére, és a továbbfejlesztések során már a tervezés fázisában kitér a technológiai továbblépés lehetőségeire, valamint figyelembe veszi az informatikai biztonság – ideértve az szolgáltatásfolytonosság – követelményeit is.

16.3. Az ügyfél adatainak, vagyonának, eszközeinek biztonsága

16.3.1. Az intézmény gondoskodik arról, hogy minden, az ügyfél által – az intézmény biztosította rendszerben – elvégzett elektronikus tranzakció esetén, amely az ügyfél adataira, pénzügyi ágazati titok körébe sorolt adataira vagy az intézmény által kezelt eszközeire, vagyonára vonatkozik, az ügyfél személye és a valódi szándéka egyértelműen azonosítható legyen.

16.3.2. Az intézmény folyamatosan monitorozza az ügyfél által elvégzett tranzakciókat, és az intézmény kockázatelemzésében meghatározott szempontok szerint gyanúsnak minősülő tranzakciókat (például szokatlan nagy összegű, vagy rövid időn belül egymástól nagy távolságra lévő helyszínekről történő utalás, vásárlás stb.) csak az ügyfél további validálását követően (például telefonos azonosítás, SMS kód) hajtja végre.

16.3.3. Az intézmény gondoskodik arról, hogy az ügyfél mindenkor általános érvényű, személyre szabott szabályokat tudjon megadni az online viselkedése, illetve szokása alapján.

16.3.4. Az elfogadó tevékenységet is folytató pénzügyi intézmény figyelemmel kíséri az internetes kereskedői tevékenységét, és a kereskedői oldalon elkövetett visszaélések észlelésére és megelőzésére csalásfelderítő rendszert működtet.

16.3.5. Az intézmény az elektronikus tranzakciókra vonatkozóan alapértelmezett értékhatárokat határoz meg, és lehetőséget biztosít az ügyfelek számára az értékhatárok módosítására.

16.3.6. Az intézmény lehetővé teszi az ügyfelek számára az egyes elektronikus szolgáltatások letiltását.

16.3.7. Az ügyfél előzetes kérése alapján az intézmény azonnali értesítéseket küld számára az általa megjelölt számlái egyenlege, valamint személyi azonosító adatai változásakor.

16.3.8. Az ügyfél számára megküldött tájékoztató vagy hitelesítő (validáló) üzenet (például SMS) küldésekor az intézmény gondoskodik arról, hogy az ügyfél számára egyértelmű legyen, hogy pontosan miről tájékoztatják, illetve, hogy pontosan milyen tranzakciót hajt végre. Ugyanakkor az üzenetet mindenkor az adattakarékosság elvének figyelembevételével szükséges megszerkeszteni.

16.3.9. Amennyiben az intézmény személyes- vagy pénzügyi ágazati titok körébe tartozó adatot nem biztonságos csatornán (például e-mail értesítés formájában) továbbít az ügyfél felé, a továbbítást megelőzően az értesítést titkosítja, és az ügyfél számára eltérő átviteli csatorna alkalmazásával a küldést megelőzően biztosítja a kódolás feloldásához szükséges alkalmazást, valamint a kulcsot.

16.3.10. Az intézmény valós idejű lehetőséget biztosít az ügyfeleknek arra, hogy a tranzakciók végrehajtási státuszát és a számlaegyenlegeket bármikor ellenőrizhessék.

16.3.11. Az intézmény az üzenetküldés letagadhatatlanságát a tranzakciós üzenetek ügyfél oldali elektronikus aláírásával és időbélyeggel biztosítja, vagy az üzenetek adott pillanatban való

meglétét érkezéskor, illetve kiküldéskor szerver oldali elektronikus aláírással és időbélyeggel igazolja.

16.3.12. Az intézmény az elektronikus tranzakciós üzeneteit hitelesíti és gondoskodik azok biztonságos őrzéséről, valamint biztosítja a vonatkozó jogszabályokban előírt ideig azok visszakereshetőségét és hitelességük igazolhatóságát.

VI. Záró rendelkezések

17. Az ajánlás az MNB tv. 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.
18. 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.
19. 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.
20. Az MNB a jelen ajánlás alkalmazását 2021. január 1-jétől várja el az érintett pénzügyi szervezetektől, azzal, hogy az MNB jó gyakorlatnak tartja, ha az újonnan kialakítandó vagy az ajánlás megjelenésekor módosítás alatt álló rendszerfejlesztéseknél már figyelembe veszik az intézmények a jelen ajánlásban foglalt elvárásokat is.
21. 2021. január 1-jén hatályát veszti a Magyar Nemzeti Banknak az informatikai rendszer védelméről szóló 7/2017. (VII. 5.) számú, valamint az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról szóló 15/2015. számú ajánlása.

Dr. Matolcsy György sk.
a Magyar Nemzeti Bank elnöke

1. melléklet a 8/2020. (VI.22.) számú MNB ajánláshoz

Tartalomjegyzék

I. AZ AJÁNLÁS CÉLJA ÉS HATÁLYA

II. TERVEZÉS, SZERVEZET, SZABÁLYOZÁS, KOCKÁZATELEMZÉS

1. Az informatikai tervezés és szervezet.....	2
1.1. Az informatikai vállalatirányítás és tervezés dokumentumai.....	2
1.2. Szervezeti és működési rend.....	3
2. Informatikai biztonsági szabályozási rendszer.....	3
2.1. Az informatikai biztonsági szabályozási rendszer alapelvei.....	3
2.2. Biztonsági osztályba sorolási rendszer.....	5
2.3. Az adatgazda és a rendszergazda kijelölését tartalmazó dokumentum.....	5
2.4. Az egyes munkakörök betöltéséhez szükséges informatikai ismeret.....	6
3. Az informatikai biztonsági kockázatelemzés, az informatikai rendszer kockázatokkal arányos védelme.....	7
3.1. Kockázatelemzés.....	7
3.2. Kockázatfelmérés.....	8
3.3. A feltárt kockázatok kezelése.....	9
3.4. A kockázatelemzés felülvizsgálata.....	9

III. BESZERZÉS, FEJLESZTÉS, TESZTELÉS, VÁLTOZÁSKEZELÉS

4. Közös rendelkezések.....	10
4.2. Beszerzés.....	10
4.3. Fejlesztés.....	11
4.4. Tesztelés, változtatáskezelés.....	12
4.5. Kiszervezés, tevékenységek kihelyezése.....	13

IV. ÜZEMELTETÉS

5. Adminisztratív védelem.....	14
5.1. A működtetésre vonatkozó szabályzatok.....	14
5.2. Szoftvereszközök nyilvántartása.....	15
5.3. Az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződések.....	16
5.4. Az informatikai rendszer elemeinek azonosítása.....	16
6. Fizikai védelem.....	16
6.1. Vonatkozó jogszabályi rendelkezés:.....	16
6.2. Általános elvárások:.....	17
7. Hálózati védelem.....	18
7.1. Vonatkozó jogszabályi rendelkezés:.....	18
7.2. Általános elvárás:.....	18

7.3. Adatkommunikációs rendszerek dokumentálása	18
7.4. Az adatok védelme távadatátvitel során	19
7.5. Határvédelem	20
7.6. Biztonsági események kezelése	21
7.7. Vírusok és más rosszindulatú kódok elleni védelem	21
7.8. Elektronikus levelezés védelme	22
8. Logikai védelem	23
8.1. Logikai védelemre vonatkozó közös rendelkezések	23
8.2. Adatbázisok biztonsága	23
8.3. Virtuális környezetek biztonsága	24
8.4. Adatátadások	24
9. Hozzáférési rend	24
9.1. Vonatkozó jogszabályi rendelkezés:	24
9.2. Hozzáférési rend szabályozása	25
9.3. Az adatokhoz való hozzáférés rendje	25
9.4. Felhasználói adminisztráció	26
9.5. Hozzáférési és felhasználói adminisztrációs szabályok ellenőrzése	28
9.6. Titkosítás, kulcskezelés, tanúsítványmenedzsment	28
10. Mentési, archiválási rendszer, helyreállítás, Adathordozók kezelése	29
10.1. Vonatkozó jogszabályi rendelkezés:	29
10.2. Általános elvárások:	30
10.3. A mentés és archiválás szabályai	30
10.4. Archiválás	31
10.5. Adathordozók kezelése	31
10.6. Mentéssel és archiválással kapcsolatos adatkezelés	32
11. Szolgáltatásfolytonosság	32
11.2. A szolgáltatásfolytonosságot akadályozó rendkívüli események kezelésére szolgáló terv	32
12. Személyi biztonság	35
12.2. Biztonságtudatosági oktatás	35
12.3. A személyi biztonság munkaügyi szabályozása	35
V. ELLENŐRZÉS	
13. Független ellenőrzés	36
13.1. Az ellenőrzés szabályai, a biztonsági rendszer ellenőrzése	36
13.2. Informatikai ellenőrző rendszer	37
14. Naplózás	38
14.1. Vonatkozó jogszabályi rendelkezés:	38
14.2. Általános elvárások:	38

14.3. Naplózás szabályozása:	38
14.4. Riasztás, azonnali reagálás:	39
14.5. Előremutató gyakorlat	39
15. Kiszervezés ellenőrzése	40
16. Az informatikai rendszer funkcionális alkalmasságának követelménye.....	40
16.1. Vonatkozó jogszabályi rendelkezés:.....	40
16.2. Általános elvárások:	40
16.3. Az ügyfél adatainak, vagyonának, eszközeinek biztonsága.....	41

2. melléklet a 8/2020. (VI.22.) számú MNB ajánláshoz

Hivatkozásmutató a Kormányrendeletre

Kormányrendelet hivatkozott szabálya	ajánlás érintett része (oldalszám)
2. § (1) bekezdése.....	2, 4, 7, 10
2. § (2) bekezdése.....	7
2. § (3) bekezdése.....	3, 36
3. § (1) bekezdése.....	17, 37
3. § (2) bekezdés a) pontja.....	16
3. § (2) bekezdés c) pontja.....	27, 38
3. § (2) bekezdés d) pontja.....	23, 38
3. § (2) bekezdés e) pontja.....	18
3. § (2) bekezdés f) pontja.....	29
3. § (2) bekezdés g) pontja.....	22
3. § (2) bekezdés b) pontja.....	36
3. § (3) bekezdés f) pontja.....	31
3. § (3) bekezdés a) pontja.....	2, 14
3. § (3) bekezdés b) pontja.....	11
3. § (3) bekezdés c) pontja.....	7, 32
3. § (3) bekezdés d) pontja.....	12
3. § (3) bekezdés e) pontja.....	29
3. § (3) bekezdés g) pontja.....	32
3. § (3) bekezdése.....	7
3. § (4) bekezdése.....	25, 29
4. § (1) bekezdés a) pontja.....	11
4. § (1) bekezdés b) pontja.....	11
4. § (1) bekezdés c) pontja.....	5
4. § (1) bekezdés d) pontja.....	25
4. § (1) bekezdés e) pontja.....	6
4. § (1) bekezdés f) pontja.....	16
4. § (1) bekezdés g) pontja.....	15
4. § (1) bekezdése.....	11
4. § (2) bekezdés e) pontja.....	23
4. § (2) bekezdése.....	40
5. §-a.....	6
5/A. § (3) bekezdés c) pont ca) alpontja.....	25
5/A. § (3) bekezdés c) pont cb) alpontja.....	38
5/A. § (3) bekezdés c) pont cc) alpontja.....	18
5/A. § (3) bekezdés c) pont cd) alpontja.....	14
5/B. § a) pontja.....	16
5/B. § b) pontja.....	14, 36
5/B. § c) pontja.....	12
5/B. § d) pontja.....	29
5/B. § e) pontja.....	25
5/B. § e) pontja.....	36
5/B. § f) pontja.....	26, 38
5/B. § g) pontja.....	27, 38
5/B. § g) pontja.....	36
5/B. § h) pontja.....	27
5/B. § h) pontja.....	36
5/B. § i) pontja.....	22
5/B. § j) pontja.....	18
5/B. § j) pontja.....	36

5/B. § k) pontja	32
5/B. § l) pontja	10
5/B. § m) pontja.....	14
5/B. § n) pontja.....	30
5/B. § n) pontja.....	36
5/B. § o) pontja.....	14
5/B. § p) pontja.....	14
5/B. § q) pontja.....	17
5/B. § r) pontja.....	18
5/B. § s) pontja	35