A Magyar Nemzeti Bank 7/2017. (VII.5.) 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 vagy közvetve alkalmas adata (a továbbiakban: ügyféladat) – illetve adó-, üzleti, bank-, értékpapír-, pénztár-, fizetési, biztosítási vagy foglalkoztatói nyugdíjtitka (a továbbiakban együtt: pénzügyi ágazati titok) védelme érdekében. Az egyes pénzügyi tevékenységekre vonatkozó ágazati törvények[1] 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 Rendelet) is rendelkezik[2].

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 Rendelet 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,

---

[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 (a továbbiakban: Fszt.) 12. § (1) bekezdés d) pontja és (3) bekezdése, valamint 12/A. §-a,
a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (a továbbiakban: Bszt.) 12. §-a,
a tőkepiacról szóló 2001. évi CXX. törvény (a továbbiakban: Tpt.) 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 (a továbbiakban: Kbftv.) 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 (a továbbiakban: Bit.) 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

hogy a kiszervezett tevékenységért való végső felelősség a megbízót terheli. Az ajánlás – e jogszabályi rendelkezéssel összhangban – a kiszervezés informatikai biztonsági vonatkozásaira is kitér.

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 az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról szóló 15/2015. MNB ajánlásban, valamint a közösségi és publikus felhőszolgáltatás igénybevételéről szóló 2/2017. (I. 12.) MNB ajánlásban foglaltakkal együtt alkalmazandó.

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.*[3] *Az intézménynek rendelkeznie kell az informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, a fejlesztésre vonatkozó tervekkel*.[4]

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 értelmezhetők, azok minden esetben – közvetlenül vagy közvetve – valamilyen üzleti folyamatot vagy annak kockázatarányos védelmét szolgálják. Ezért az intézmény az üzleti stratégiájára alapozva meghatározza az informatikai vállalatirányítás és tervezés szabályzatait, az alábbiak szerint:

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

a) informatikai stratégia,

b) éves informatikai beruházási és költség tervek.

[3] Bszt. 12. § (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Rendelet 2. § (1) bekezdése

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

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*.[5]

1.2.2. Az intézmény az informatikai szervezetének felépítését és működését a szervezeti és működési szabályzatában rögzíti, és az informatikai munkakörökhöz rendeli a feladatokat és felelősségeket 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.

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

2. INFORMATIKAI BIZTONSÁGI SZABÁLYOZÁSI RENDSZER

2.1. Az informatikai biztonsági szabályozási rendszer alapelvei

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.*[6]

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

[5] Bszt. 12. § (4) bekezdése, Mpt. 77/A. § (3) bekezdése, Öpt. 40/C. § (3) bekezdése, Rendelet 2. § (3) bekezdése
[6] Bszt. 12. § (1) és (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Rendelet 2. § (1) bekezdése

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 teljes körűsége és folyamatos megfelelősége az intézménynél elvárt magatartás és teljesítés számonkérésének alapja.

2.1.4. Az informatikai biztonsági szabályozási rendszer kialakításakor az intézmény gondoskodik arról, hogy a szabályzati 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-, információs 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 kockázatelemzése előírt aktualizálásához kapcsolódóan.

2.1.8. A szabályozási rendszer elemeinek rendelkezései egyértelműek, világosak, könnyen érthetők, betarthatók és betartathatók.

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 a szabályozásnak mindenkor az intézmény működéséhez kell illeszkednie. Nem célszerű a szabályozásban olyan gyakorlatokat előírni, amelyek az intézmény szempontjából nem relevánsak, nem életszerűek, technikailag kivitelezhetetlenek, a kockázatokkal nem állnak arányban, betarthatatlanok, vagy egyszerűbb kompenzáló kontrollokkal költségarányosabb módon helyettesíthetők.

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*.[7]

2.2.2. Az adatgazda adatbiztonsági osztályokba sorolja az adatokat, bizalmasságukat, sértetlenségüket és rendelkezésre állásukat veszélyeztető 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, az ezekből – visszafejthető módon – származtatott adatokat, valamint az ezeket feldolgozó rendszereket és infrastruktúra elemeket a legszigorúbb biztonsági osztályba sorolja.

2.2.6. Amennyiben az intézmény a minősített adat védelméről szóló törvény szerinti minősített adatok kezelésére jogosult, és ezen adatokat is figyelembe veszi a biztonsági osztályba sorolás során, úgy a 2.2.5. pontban foglalt legszigorúbb biztonsági osztályt a minősített adatokat tartalmazó osztályt követő legszigorúbb biztonsági osztályként kell értelmezni.

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*.[8]

2.3.2. Az adatgazda és a rendszergazda fontos szereplői az információbiztonság kikényszerítésének. Az adatgazda az ágazati jogszabályokban foglaltak figyelembe vételével meghatározza a rá bízott adatok bizalmasságának, 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.

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

[8] Bszt. 12. § (9) bekezdés e) pontja, Mpt. 77/A. § (7) bekezdés e) pontja, Öpt. 40/C. § (7) bekezdés e) pontja, Rendelet 4. § (1) bekezdés e) pontja

2.3.3. Az intézmény rendelkezik az adatgazdák és a rendszergazdák feladatairól, felelősségeiről, kijelölésük és feladataik ellátásának eljárásrendjéről, ezek dokumentálásáról.

2.3.4. Az intézmény az adatgazda feladataként 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 számonkérhetően 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 felelősségeikről.

2.3.7. Az intézmény gondoskodik annak igazolhatóságáról, hogy az adatgazdák és rendszergazdák elfogadták kijelölésüket, feladataikat és felelősségeiket.

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 ismeretet meghatározó dokumentumok

2.4.1. **Vonatkozó jogszabályi rendelkezés:** *az intézmény a belső szabályzatában meghatározza az egyes munkakörök betöltéséhez szükséges informatikai ismeretet*.[9]

2.4.2. Az intézmény gondoskodik arról, hogy a munkatársak a megfelelő ismeretek birtokában képesek legyenek az üzleti folyamatok során kezelt adatok bizalmasságát, 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.

[9] Bszt. 12. § (11) bekezdése, Mpt. 77/A. § (9) bekezdése, Öpt. 40/C. § (9) bekezdése, Rendelet 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.*[10] *Az intézmény az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétévente felülvizsgálja és aktualizálja.*[11] *Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja".*[12]

Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.[13]

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) vállalatirányítás,
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.

[10] Bszt. 12. § (1) és (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Rendelet 2. § (1) bekezdése
[11] Bszt. 12. § (3) bekezdése, Mpt. 77/A. § (2) bekezdése, Öpt. 40/C. § (2) bekezdése, Rendelet 2. § (2) bekezdése
[12] Bszt. 12. § (7) bekezdése, Mpt. 77/A. § (6) bekezdése, Öpt. 40/C. § (6) bekezdése, Rendelet 3. § (3) bekezdése
[13] Rendelet 5/A. § (3) bekezdés c) pontja

3.1.5. A vonatkozó jogszabályok nem szabályozzák a kockázatfelmérés elvégzésének módját (módszertanát, eljárásait, lépéseit), erről az intézmény szabadon dönt. A kockázatfelmérésnek az intézmény sajátosságait kell elsősorban figyelembe vennie, ezért az általános érvényű kockázatfelmérési 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 teljes körűen azonosítja és értékeli informatikai rendszerének biztonsági kockázatait az informatikai biztonsággal érintett valamennyi területen (informatikai vállalatirányítás, 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 bizalmasságának, 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 rendszerelemek, 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 rendszerelemekhez, 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 rendszerelemekhez 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, katalógusokat[14] és bevált gyakorlatokat;

g) a szabályzati előírások és a gyakorlat összhangjának a vizsgálata;

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 teljes körűen 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 kockázatokat, amelyeket az intézmény nem kezel, dokumentáltan felvállalja. Az intézmény nem vállalhat fel jogszabályi rendelkezések betartásával kapcsolatos kockázatokat.

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 időpontján.

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

[14] pl. COBIT5, MSZ/T ISO/IEC 27001:2014, BSI IT-Grundschutz-Kataloge

eredményét megismerte, és a feltárt, de az intézkedési tervben nem szereplő kockázatokat 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 kockázatokat 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 releváns jogszabályokban vagy szabályozási rendben bekövetkezett változás esetén az intézmény a változással érintett területen haladéktalanul aktualizálja kockázatelemzését.

3.4.2. Az intézmény kétévente vagy annál gyakrabban az informatikai biztonságot érintő valamennyi területen, teljes körűen 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.*[15]

4.1.2. Az intézmény a szolgáltatási vagy kiegészítő szolgáltatási tevékenysége ellátásával kapcsolatos rendszerek és szolgáltatások beszerzésével, fejlesztésével megbízhat külső vállalkozókat. Az intézmény a beszerzett rendszerekért, tevékenységekért és fejlesztésekért a felelősséget maga viseli. 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*.[16]

4.2.2. Az intézmény az informatikai szabályozási rendszerében rendelkezik a beszerzés szabályairól és eljárásrendjéről.

[15] Bszt. 12. § (1) és (2) bekezdése, Mpt. 77/A. § (1) bekezdése, Öpt. 40/C. § (1) bekezdése, Rendelet 2. § (1) bekezdése

[16] Rendelet 5/B. § l) pontja

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**

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.*[17] *Az intézménynél mindenkor rendelkezésre kell állnia az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek, valamint az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének.*[18]

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

a) áttekinthető formában elkészül;

b) tartalmazza a rendszer felépítésének és működtetésének ellenőrzéséhez szükséges rendszerleírásokat és modelleket, valamint az adatok szintaktikai szabályait és tárolási szerkezetét (például 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

[17] Bszt. 12. § (7) bekezdés b) pontja, Mpt .77/A. § (6) bekezdés b) pontja, Öpt. 40/C. § (6) bekezdés b) pontja, Rendelet 3. § (3) bekezdés b) pontja

[18] Bszt. 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, Rendelet 4. § (1) bekezdés a) és b) pontja a) b)

információ a dokumentált adatszerkezet, objektum, funkció, modul, program, egyéb rendszerkomponens szerepéről és működéséről);

c) 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;

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, teljes körűen fordítható vagy fordítás nélkül futtatható állapotú, egyértelműen azonosított és aktuális) forráskód állományához és fejlesztési dokumentációjához, és azok felett a továbbiakban jogszerűen rendelkezhessen.

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 figyelembe vételével, további felhasználásra alkalmas formátumban – mindenkor a rendelkezésére álljanak.

4.3.5. ***Előremutató gyakorlat***

Az intézmény gondoskodik arról, hogy az informatikai biztonságért felelős személy vagy szervezet már a fejlesztések tervezésétől kezdődően (by design), azok teljes életciklusába folyamatosan bevonásra kerüljön.

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.*[19] *Az élesüzemi rendszer változáskezelési folyamatai biztosítják, hogy a rendszer paraméterezésében és a szoftverkódban bekövetkező változások csak tesztelt és dokumentált módon valósulhatnak meg.*[20]

4.4.2. Adatkezelőként mindenkor biztosítani kell 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 gondoskodni kell arról, 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

[19] Bszt. 12. § (7) bekezdés d) pontja, Mpt. 77/A. § (6) bekezdés d) pontja, Öpt. 40/C. § (6) bekezdés d) pontja, Rendelet.3. § (3) bekezdés d) pontja

[20] Rendelet 5/B. § c) pontja

rendelkezésre állási szempontú szeparációjáról gondoskodni, az adatokat meg kell fosztani azoktól a jellemzőktől, amelyek okán bizalmasnak minősülnek. Így különösen: az ügyféladatot és a pénzügyi ágazati titok körébe tartozó adatokat felismerhetetlenné kell tenni 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 üzemi környezettől elkülönített környezetekben végzi.

4.4.5. Az intézmény nem, vagy csak teljeskörű anonimizálást követően használ éles rendszerből vett adatokat a fejlesztői és teszt környezetben.

4.4.6. A futtatható kód éles üzembe állítását az intézmény informatikai üzemeltetője végzi, aki egyben gondoskodik a forrás- és a futtatható kód azonosításáról és tárolásáról, valamint a tesztelt, az élesítésre jóváhagyott és az élesüzembe állított verziók azonosságának ellenőrzéséről.

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 teszteket is.

4.4.9. **Előremutató gyakorlat**

Az intézmény gondoskodik a fejlesztési és a teszt környezet elkülönítéséről is.

4.5. Kiszervezés

4.5.1. Az intézmény a kiszervezett tevékenységért ugyanúgy felel, mint ha azt önmaga 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 kiszervezésként való kezelésével biztosítja a szolgáltatás – az intézmény, illetve az MNB általi – megfelelő ellenőrizhetőségét és átlátható működését.

4.5.2. A kiszervezés során az intézmény gondoskodik arról, hogy az ügyféladathoz, 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 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 az intézmény gondoskodik az érintettek megfelelő tájékoztatásáról, hogy az ügyféladat, 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 tevékenységet végző (szolgáltató) szerződésben rögzítik:

a) a szolgáltató által minimálisan elkészítendő és betartandó szabályzatokat,
b) a szolgáltató informatikai biztonsági feladatait és felelősségét, ezen belül a kiszervezett 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 mindenkori alkalmazhatóságára,
f) ezen eljárások tesztelésének módszerét, gyakoriságát, valamint az intézmény felé történő beszámolás módját.

4.5.6. **Előremutató gyakorlat**

Az intézmény minden olyan tevékenységét, amely során harmadik fél az ügyfél adataihoz vagy az ügyfél közvetett azonosítására alkalmas adatokhoz bármilyen módon hozzáférhet— függetlenül attól, hogy ezt milyen minőségében és jogalappal teszi –célszerű kiszervezésként kezelni. Ezzel az intézmény proaktív módon biztosítja a transzparenciát a harmadik személyek ügyféladathoz (adott esetben személyes vagy különleges adathoz), illetve pénzügyi ágazati titok körébe tartozó adathoz történő hozzáférései vonatkozásában.

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.*[21] *Az intézmény élesüzemi rendszere üzemeltetési folyamatai szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek;*[22] *az élesüzemi rendszer karbantartása szabályozott, és megfelel a rendelkezésre állásra vonatkozó elvárásoknak,*[23] *az élesüzemi rendszer és az üzemeltetési szabályzatok gondoskodnak a rendszerelemek és a kezelt információk sértetlenségéről,*[24] *az élesüzemi rendszer és az üzemeltetési szabályzatok*

[21] Bszt. 12. § (7) bekezdés a) pontja, Mpt. 77/A. § (6) bekezdés a) pontja, Öpt. 40/C. § (6) bekezdés a) pontja, Rendelet 3. § (3) bekezdés a) pontja
[22] Rendelet 5/B. § b) pontja
[23] Rendelet 5/B. § m) pontja
[24] Rendelet 5/B. § o) pontja

gondoskodnak a rendszer és a kommunikáció kellő szintű védelméről[25]*. A szabályozások és eljárások garantálják a rendszer biztonsági szintjének folyamatos fenntartását, a szoftverek frissítését, üzemeltetését.*[26]

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 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 operatív utasításoknak együttesen alkalmasnak kell lenniük 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 kockázatelemzése 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.

[25] Rendelet 5/B. § p) pontja

[26] Rendelet 5/A. § (3) bekezdés c) pont cd) alpontja

5.1.8. **Előremutató gyakorlat**

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.*[27]

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 hálózatból nem érhetők el.

5.2.5. Előremutató gyakorlat

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.*[28]

5.3.2. Az intézmény rendelkezik az általa birtokolt 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.

5.4. 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*

[27] Bszt.12. § (9) bekezdés g) pont, Mpt. 77/A. § (7) bekezdés g) pont, Öpt. 40/C. § (7) bekezdés g) pont, Rendelet 4. § (1) bekezdés g) pont

[28] Bszt. 12. § (9) bekezdés f) pontja, Mpt. 77/A. § (7) bekezdés f) pontja, Öpt. 40/C. § (7) bekezdés f) pontja, Rendelet 4. § (1) bekezdés f) pontja

visszakereshető azonosításáról.[29] *Az intézmény biztosítja, hogy az élesüzemi rendszer elemei azonosíthatóak és dokumentáltak.*[30]

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

a) az eszköz megnevezése, típusa, azonosítója,

b) az eszköz aktuális elhelyezése – tárolási helye, vagy mobil eszközök esetében a használó személye,

c) az eszköz hardver és szoftver konfigurációja.

5.4.3. A nyilvántartás 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: az intézmény kiépíti az informatikai rendszere biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működteti,[31] megfelelő szintű fizikailag védett környezetet biztosít az élesüzemi rendszer számára[32].

6.2. A szolgáltatásfolytonosság valamint az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében az adminisztratív és a logikai biztonságon felül gondoskodni kell 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 rácsozás kialakítása).

[29] Bszt. 12. § (6) bekezdés a) pontja, Mpt. 77/A. § (5) bekezdés a) pontja, Öpt. 40/C. § (5) bekezdés a) pontja, Rendelet 3. § (2) bekezdés a) pontja

[30] Rendelet 5/B. § a) pontja

[31] Bszt. 12. § (5) bekezdése, Mpt. 77/A. § (4) bekezdése, Öpt. 40/C. § (4) bekezdése, Rendelet 3. § (1) bekezdése

[32] Rendelet 5/B. § q) pontja

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

a) tápáramellátás (akadozás, ingadozás, kimaradás),

b) üzemitől 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 gondoskodik a kritikus infrastruktúra elemeket tároló helyiségek tűzvédelméről.

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.

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

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

6.2.9. Előremutató gyakorlat

6.2.9.1. 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.

6.2.9.2. 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.*[33] *Az intézmény biztosítja, hogy az élesüzemi rendszer adatkommunikációs és rendszerkapcsolatai dokumentáltak és ellenőrzöttek annak érdekében, hogy az adatkommunikáció bizalmassága, sérthetetlensége és*

[33] Bszt. 12. § (6) bekezdés e) pontja, Mpt. 77/A. § (5) bekezdés e) pontja, Öpt. 40/C. § (5) bekezdés e) pontja, Rendelet 3. § (2) bekezdés e) pontja

hitelessége biztosítható legyen[34], a szervezet detektálja és kezeli az egyes biztonsági eseményeket.[35] Az informatikai rendszer összes külső interfésze szabályozott és kontrollált.[36]

7.2. Az adatkommunikációs, rendszerkapcsolati és hálózati dokumentációknak együttesen alkalmasnak kell lenniük 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) a kapcsolatok típusát és jellegét is feltüntető adatkapcsolati ábra,

b) hálózati topológia ábra,

c) géptermi elhelyezési rajzok,

d) hálózati zónák és átjárási szabályok leírása.

7.4. Az adatok védelme távadatátvitel során

7.4.1. Az intézmény az ügyfél 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 ügyféladatot vagy pénzügyi ágazati titok körébe tartozó adatot továbbíthat, illetve amelyek az intézmény adathálózatára csatlakoznak.

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

[34] Rendelet 5/B. § j) pontja

[35] Rendelet 5/B. § r) pontja

[36] Rendelet 5/A. § (3) bekezdés c) pont cc) alpontja

7.5. Határvédelem

7.5.1. A hálózati kapcsolatokat úgy kell kialakítani, hogy azokon mindenkor csak az üzletileg indokolt és engedélyezett forgalom haladjon át. Ennek érdekében

7.5.2. Az intézmény gondoskodik a megfelelően szabályozott, üzleti igényekkel alátámasztott, engedélyezett, dokumentált, és rendszeresen – de legkésőbb a kockázatelemzése során – felülvizsgált hálózati kapcsolati szabályrendszerről.

7.5.3. Az intézmény az engedélyezett kapcsolati szabályokat megfelelő határvédelmi megoldások használatával technológiailag is kikényszeríti.

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.

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 szabályok, szabályrendszerek, támadási minták, határvédelmi eszközök és -szoftvertermékek folyamatos felülvizsgálatáról és tervezett frissítéséről.

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 IT működést akadályozó incidensekről és azok megoldásáról.

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.*[37] *Az intézménynél az élesüzemi rendszer vírus és más rosszindulatú programok elleni védelme biztosított*.[38]

7.7.2. Az intézmény az informatikai rendszere elemein a vírusok és más rosszindulatú kódok kiszűrésére alkalmas programot működtet, valamint biztosítja a program naprakész állapotát és naplózását.

[37] Bszt. 12. § (6) bekezdés g) pontja, Mpt. 77/A. § (5) bekezdés g) pontja, Öpt. 40/C. § (5) bekezdés g) pontja, Rendelet 3. § (2) bekezdés g) pontja

[38] Rendelet 5/B. § i) pontja

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.

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 az informatikai rendszereiben csak olyan szoftvertermékeket és rendszerprogramokat futtasson, amelyek rendelkeznek terméktámogatással és biztonsági frissítéssel, ezzel is csökkentve az ismert szoftverhiányosságok kihasználásával történő rosszindulatú kódok bejuttatásának kockázatát.

7.7.6. **Előremutató gyakorlat**

7.7.6.1. Az intézmény a kockázataival arányosan gondoskodhat többrétegű, mélységi védelemről.

7.7.6.2. Az intézmény központi kezelő felülettel rendelkező végponti biztonsági programot működtet.

8. ADATHORDOZÓK KEZELÉSE

8.1. Vonatkozó jogszabályi rendelkezés: az intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell az adathordozók szabályozott és biztonságos kezeléséről.[39] Az intézménynél az élesüzemi rendszer adathordozóinak védelme szabályozott, megfelelően korlátozott, és a korlátozásokat rendszeres felülvizsgálatokkal és ellenőrzésekkel is fenntartják.[40]

8.2. Adathordozó minden olyan eszköz vagy rendszerelem, amely alkalmas az adatok tárolására.

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

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

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

8.6. Előremutató gyakorlat

8.6.1. Az intézmény megfontolja és kockázatai alapján döntést hoz az adathordozók egyedi nyilvántartásának a bevezetéséről.

[39] Bszt.12.§ (6) f), Mpt.77/A.§ (5) f), Öpt.40/C.§ (5) f), Rendelet 3. § (2) f)
[40] Rendelet 5/B. § n)

8.6.2. Az intézmény a kockázataival arányosan gondoskodhat az adathordozókon tárolt adatok titkosításáról.

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.[41] Az intézménynél mindenkor rendelkezésre kell állnia az adatokhoz történő hozzáférési rend meghatározásának,[42] valamint az intézménynek gondoskodnia kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.[43] A jogosult általános (emberek és program entitások) és privilegizált (speciális jogokkal felruházott) felhasználók – így különösen rendszergazdák – kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhetnek a védendő információkhoz és az azokat kezelő rendszer elemeihez, kezdeményezhetnek aktivitásokat, valamint kizárólag meghatározott privilegizált felhasználók adhatnak szabályozott szerepkörüknek megfelelően és ellenőrzött módon hozzáférési jogosultságokat.[44]

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 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.

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.

[41] Rendelet 5/B. § e) pontja
[42] Bszt. 12. § (9) bekezdés d) pontja, Mpt. 77/A. § (7) bekezdés d) pontja, Öpt. 40/C. § (7) bekezdés d) pontja, Rendelet 4. § (1) bekezdés d) pontja
[43] Bszt. 12. § (8) bekezdése, Mpt. 77/A. § (6) bekezdés e) pontja, Öpt. 40/C. § (6) bekezdés e) pontja, Rendelet 3. § (4) bekezdése
[44] Rendelet 5/A. § (3) bekezdés c) pont ca) alpontja

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) megszemélyesítenek.

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.

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 – 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 (pl. 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 (pl. 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 (pl. jelszószabályok, naplózási beállítások),

i) a kiemelt jogosultságú rendszer fiókok (pl. 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;*[45] *az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek, továbbá a kiemelt jogosultságokkal elvégzett tevékenység naplózása megvalósul, a napló fájlok sérthetetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak;*[46] *az élesüzemi rendszerhez történő távoli hozzáférés szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött*[47]*. 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).*[48]

9.4.2. Az intézmény az informatikai rendszeréhez való hozzáférést 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.

[45] Rendelet 5/B. § f) pontja

[46] Rendelet 5/B. § g) pontja

[47] Rendelet 5/B. § h) pontja

[48] Bszt.12. § (6) bekezdés c) pontja, Mpt. 77/A. § (5) bekezdés c) pontja, Öpt. 40/C. § (5) bekezdés c) pontja, Rendelet 3. § (2) bekezdés c) pontja

9.4.6. Az intézmény a jelszó komplexitási és lejárati szabályokat az egyes rendszerekben a felhasználói fiókok használatával végezhető tevékenységek kockázataival arányosan, a felhasználók által kezelhető módon határozza meg.

9.4.7. Az ügyféladatot 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. A kritikus rendszerek esetében az intézmény a felhasználói fiók be- és kilépés, jelszóváltoztatás események adatait – kivéve a jelszót – naplózza.

9.4.9. Távoli hozzáférések esetében az intézmény a felhasználói fiók mellett legalább még egy további, a felhasználót hitelesítő faktort – pl. dinamikus kódot, tanúsítványt – is használ.

9.4.10. Amennyiben az intézmény PKI rendszert üzemeltet és tanúsítványokat állít elő, rendelkezik a kapcsolódó, dokumentált kulcskezelési eljárással.

9.4.11. 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 megfelelőségének időszakos ellenőrzését.

9.4.12. **Előremutató gyakorlat**

Az intézmény a kockázataival arányos módon gondoskodik az informatikai rendszereiben a jelszóra vonatkozóan az alábbi szabályok bevezetéséről:

a) a jelszó minél több (min. 12) 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 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) exponenciálisan növekednek.

9.5. Hozzáférési és felhasználói adminisztrációs szabályok ellenőrzése

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 ellenőrzésével meggyőződik a hozzáférési és felhasználói adminisztrációs szabályok betartásáról.

10. MENTÉSI, ARCHIVÁLÁSI RENDSZER, HELYREÁLLÍTÁS

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.[49] Az élesüzemi rendszer adatmentési és visszaállítási rendje biztosítja a rendszer biztonságos visszaállítását, továbbá a mentés-visszaállítás a vonatkozó szabályzat szerinti gyakorisággal és dokumentáltan tesztelt[50].

10.2. 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 intézménynek az archiválások során biztosítania kell, hogy az adatok egy későbbi időpontban is visszaállíthatók legyenek, ezért gondoskodnia kell az erre alkalmas technológiák és megoldások alkalmazásáról. Ennek érdekében:

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 figyelembe vételével úgy alakítja ki, hogy a mentések típusa, gyakorisága és példányszáma elfogadható idő- és adatveszteségi 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 – pl. adatmegőrzési idő, újraírhatóság száma, tárolási előírások – figyelembe vételével történjen;

d) a mentéseket és archív adatokat tartalmazó adathordozók kezelése a rajtuk tárolt adatok biztonsági osztályához rendelt előírások szerint történjen;

[49] Bszt. 12. § (7) bekezdés e) pontja és (8) bekezdése, Mpt. 77/A. § (6) bekezdés e) pontja, Öpt. 40/C. § (6) bekezdés e) pontja, Rendelet 3. § (3) bekezdés e) pontja és (4) bekezdése

[50] Rendelet 5/B. § d) pontja

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.

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.

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 (pl. 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 megfelelősségének 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 megőrizzék.*[51]

10.4.2. Az intézmény a jogszabályban meghatározott nyilvántartásairól a dokumentált mentési rend alapján mentéseket készít, és azokat az ágazati jogszabályokban meghatározott ideig – de 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. Mentéssel és archiválással kapcsolatos adatkezelés

10.5.1. 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. A mentések kialakítása során biztosítani kell, hogy az ügyféladatok és a pénzügyi ágazati titok körébe tartozó adatok a csak a jogszabályi előírások szerinti időtartamában kerüljenek tárolásra. Ezt követően az adatokat törölni kell, vagy az adatok ügyféllel történő összekapcsolását visszaállíthatatlanul meg kell szüntetni úgy, hogy az ügyféladat és a pénzügyi ágazati titok körébe tartozó adat az érintettel a továbbiakban ne legyen összefüggésbe hozható, a kapcsolat közöttük ne legyen helyreállítható.

10.5.2. A mentések és archív állományok tárolása és kezelése során biztosítani kell az adathordozókra vonatkozó szabályok (lásd 8.1. 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).*[52] *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*

[51] Bszt. 12.§ (7) bekezdés f) pontja, Mpt. 77/A. § (6) bekezdés f) pontja, Öpt. 40/C. § (6) bekezdés f) pontja, Rendelet 3. § (3) bekezdés f) pontja

[52] Bszt. 12. § (7) bekezdés g) pontja, Mpt. 77/A. § (6) bekezdés g) pontja, Öpt. 40/C. § (6) bekezdés g) pontja, Rendelet 3. § (3) bekezdés g) pontja

tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal .[53] *A katasztrófa-helyreállítási terv rendszeresen tesztelt.*[54]

11.2. A szolgáltatásfolytonosságot akadályozó rendkívüli események kezelésére szolgáló terv

11.2.1. A szolgáltatásfolytonossági tervnek biztosítani kell az üzletszabályzatban és az aktuális hirdetményekben közzétett működési feltételeket.

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, 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.

[53] Bszt. 12. § (7) bekezdés c) pontja, Mpt. 77/A.§ (6) bekezdés c) pontja, Öpt. 40/C. § (6) bekezdés c) pontja, Rendelet 3. § (3) bekezdés c) pontja

[54] Rendelet 5/B. § k) pontja

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 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 során a szolgáltatásfolytonossági tervet felülvizsgálja, valamint dokumentáltan teszteli 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 tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb megoldásokkal. Ennek érdekében az intézmény

a) szolgáltatásai folytonosságát biztosító tartalék berendezések alkalmasak az élesüzemi berendezések meghibásodásakor automatikusan vagy manuális közreműködéssel RTO időn belül RPO szerinti szolgáltatási pontról 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 tartalék berendezéseket 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 tűzeset, földrengés, árvíz, tűzszerészeti 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 meg kell haladja 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.

11.2.8. **Előremutató gyakorlat**

A szolgáltatásfolytonossági tervezés során az alábbiak figyelembevétele 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 biztonságtudatossági oktatáson vesznek részt, valamint az intézmény dolgozóinak munkaügyi szabályozása megfelel a biztonsági előírásoknak.*[55]

12.2. Biztonságtudatossági oktatás

12.2.1. Az intézmény az informatikai biztonsági szabályozási rendszerében meghatározza az informatikai biztonságtudatossági 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, dokumentált biztonságtudatossági oktatásáról.

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

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 (adathozzáférésének) változásával kapcsolatos biztonsági eljárásrendet.

[55] Rendelet 5/B. § s) pontja

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.*[56] *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, eljárásokról*[57]*; az élesüzemi rendszer üzemeltetési folyamatai szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek*[58]*; az élesüzemi rendszerhez való végfelhasználói hozzáférés mind alkalmazási, mind pedig infrastruktúra szinten szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött*[59]*; az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzöttek*[60]*; az élesüzemi rendszerhez történő távoli hozzáférés szabályozott, dokumentált és a vonatkozó szabályzat szerinti gyakorisággal ellenőrzött* [61]*; az élesüzemi rendszer adatkommunikációs és rendszerkapcsolatai dokumentáltak és ellenőrzöttek annak érdekében, hogy az adatkommunikáció bizalmassága, sérthetetlensége és hitelessége biztosítható legyen* [62]*; az élesüzemi rendszer adathordozóinak védelme szabályozott, megfelelően korlátozott, és a korlátozásokat rendszeres felülvizsgálatokkal és ellenőrzésekkel is fenntartják*[63]*.*

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, implemetálásába vagy azok működtetésébe, és nincs alárendelt viszonyban az ellenőrzött területtel.

13.1.3. Az intézmény gondoskodik az informatikai biztonság – szabályzatban meghatározott – független és rendszeres ellenőrzéséről.

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;

---

[56] Bszt. 12. § (4) bekezdése, Mpt. 77/A. § (3) bekezdése, Öpt. 40/C. § (3) bekezdése, Rendelet 2. § (3) bekezdése

[57] Bszt. 12. § (6) bekezdés b) pontja, Mpt. 77/A. § (5) bekezdés b) pontja, Öpt. 40/C. § (5) bekezdés b) pontja, Rendelet 3. § (2) bekezdés b) pontja

[58] Rendelet 5/B. § b) pontja

[59] Rendelet 5/B. § e) pontja

[60] Rendelet 5/B. § g) pontja

[61] Rendelet 5/B. § h) pontja

[62] Rendelet 5/B. § j) pontja

[63] Rendelet 5/B. § n) pontja

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 szabályozásban 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 bizalmasságának, sértetlenségének és hitelességének biztosítására és ellenőrizhetőségére;
e) az adathálózati sérülékenység vizsgálat évente, a bankkártya rendszerek vonatkozásában legalább negyedévente ismételve, valamint a kockázatként meghatározott hibák javítása megtörténik;
f) internet felől elérhető alkalmazások sérülékenység vizsgálata a kockázatként meghatározott hibák javítása, üzembe állítást megelőzően, majd legalább 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 üzemet követően a gyártói javító csomagok installálása 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 fentieken 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.*[64]

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 időknek megfelelően megtörténhessen. Ennek biztosítása érdekében az intézmény:

a) felhasználói támogató szervezetet üzemeltet;

b) a 6.2.2. pontban foglaltaknak megfelelő automatikus rendszerfelügyeleti és riasztó rendszert működtet;

[64] Bszt. 12. § (5) bekezdése, Mpt. 77/A. § (4) bekezdése, Öpt. 40/C. § (4) bekezdése, Rendelet 3. § (1) bekezdése

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.*[65] *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.*[66] *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.*[67] *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 sérthetetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak.*[68]

14.2. 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 sértetlenségét, folyamatosan gondoskodik a naplókiértékelésről, a naplózási szabályok betartását technológiai megoldásokkal is kikényszeríti.

14.3. 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 operatív utasításai elkészítését, dokumentálását és felülvizsgálatát az informatikai biztonsági szabályozási rendszerben szabályozza;

[65] Bszt. 12. § (6) bekezdés d) pontja, Mpt. 77/A. § (5) bekezdés d) pontja, Öpt. 40/C. § (5) bekezdés d) pontja, Rendelet 3. § (2) bekezdés d) pontja

[66] Rendelet 5/A. § (3) bekezdés c) pont cb) alpontja

[67] Bszt. 12. § (6) bekezdés c) pontja, Mpt. 77/A. § (5) bekezdés c) pontja, Öpt. 40/C. § (5) bekezdés c) pontja, Rendelet 3. § (2) bekezdés c) pontja

[68] Rendelet 5/B. § f) pontja és g) pontja

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 értesítendők körét, az azonnali riasztás eseteit és módját.

14.4. 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.

14.5. Az intézmény a naplózás szabályozási rendszerében meghatározottakat technológiai megoldásokkal is kikényszeríti.

14.6. Előremutató gyakorlat

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

14.6.2. 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.

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

15. KISZERVEZÉS ELLENŐRZÉSE

15.1. A kiszervezett tevékenység szerződésben foglaltaknak megfelelő ellátását az intézmény a kiszervezési szerződésben, valamint az ágazati törvényekben[69] meghatározott módon és rendszerességgel ellenőrzi.

15.2. 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.

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

15.3. 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.

15.4. 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 cégbíróság felé történő bejelentését is, a tárolt adatok ellenőrzéséhez való felhasználására, valamint a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.*[70]

16.2. Az intézmény alkalmazási rendszerei eleget tesznek a vonatkozó pénzügyi-számviteli jogszabályi előírásoknak, így különösen

a) a pénzügyi tranzakciókat szigorúan naplózott módon, idősorosan vezeti (ahol az idősorrend – 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,

b) az üzleti és a biztonsággal kapcsolatos tranzakciókat egyaránt naplózza,

c) 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;

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

16.3. 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.

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

[70] Bszt.12.§ (10) bekezdése, Mpt.77/A.§ (8) bekezdése, Öpt.40/C.§ (8) bekezdése, Rendelet 4. § (2) bekezdése

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 2017. július 15-től várja el az érintett pénzügyi szervezetektől.

21. 2017. július 15-én hatályát veszti a Magyar Nemzeti Banknak az informatikai rendszer védelméről szóló 1/2015. számú ajánlása.

Dr. Matolcsy György sk.
a Magyar Nemzeti Bank elnöke

1. melléklet a 7/2017. (VII.5.) számú MNB ajánláshoz

Hivatkozásmutató a Rendelethez