33/2021. (IX. 15.) MNB rendelet

a fizetési rendszer működtetése tevékenységre vonatkozó részletes szabályokról

A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 171. § (2) bekezdés *d)* pontjában és (3) bekezdés *a)* pontjában kapott felhatalmazás alapján, a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 4. § (5) bekezdésében, valamint 28. § (1) és (2) bekezdésében meghatározott feladatkörömben eljárva a következőket rendelem el:

1. Általános rendelkezések

1. § (1) A rendelet hatálya a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény (a továbbiakban: Hpt.) szerinti fizetési rendszer működtetése tevékenységet végző szervezetre terjed ki.

(2) E rendeletet a fizetési rendszer működtetése tevékenység tekintetében - a 3. § (2) bekezdés, (3) bekezdés *b)*, *c)* és *d)* pontja, (4) bekezdés, a 10. §, a 11. § és a 12. § kivételével - a Magyar Nemzeti Bankra (a továbbiakban: MNB) is alkalmazni kell.

(3) E rendelet 15. § (5) bekezdésében, 21. § (1) és (5) bekezdésében, 22. §-ában, 23. § (1)-(4), (6) és (7) bekezdésében foglalt rendelkezéseknek való megfelelést a rendszerüzemeltető a fizetési rendszer valamennyi teljesértékű helyszíne tekintetében köteles biztosítani.

(4) Amennyiben a rendszerüzemeltető és a teljesítő fél a fizetési rendszer működtetéséhez szükséges egyes tevékenységeinek ellátásához külső szolgáltatót vesz igénybe, a külső szolgáltatóval együttesen biztosítja a rendelet szabályainak történő megfelelést.

2. § E rendelet alkalmazásában

1. *akcióterv:* a krízishelyzetre való felkészülési feltételeket, a krízishelyzetre vonatkozó válaszlépéseket, az alternatív, továbbá visszaállítási és ellenőrző eljárásokat tartalmazó terv;

2. *általános üzleti kockázat:* a rendszerüzemeltető pénzügyi helyzetében üzleti szempontból bekövetkezett potenciális romlás a bevételeinek csökkenése vagy a költségeinek emelkedése következtében, amely esetben a költségei meghaladják a bevételeit, és ennek eredményeképpen a veszteséget tőkéből kell fedeznie;

3. *áttelepülés:* a fizetési rendszer működtetéséhez kapcsolódó tevékenységek egészének vagy egyes részeinek másik teljesértékű helyszínen való végzése érdekében megtett intézkedés;

4. *belső kontroll funkció:* a kockázatkezelési funkció, a megfelelőség biztosítási funkció és a belső ellenőrzési funkció együttesen;

5. *biztonsági rendszer:* a logikai biztonság részét képező informatikai termékek és megoldások összessége;

6. *együttműködő felek:* a fizetési rendszer működtetéséről szóló megállapodásban részes intézmények, azaz a rendszerüzemeltető, a közvetlen résztvevő, a közvetlen benyújtó, a teljesítő fél, valamint egyéb, a fizetési rendszer üzletszabályzatában ilyenként nevesített fél;

7. *elektronikai védelem:* a rendszerüzemeltető elhelyezésére szolgáló épület (épületrész), valamint a védendő helyiségek illetéktelen behatolás elleni fokozott védelmét és megfigyelését támogató elektronikus vagyonvédelmi rendszerek összessége;

8. *elektronikus vagyonvédelmi rendszer:* elektronikus jelző-, illetve képi megfigyelőrendszer, továbbá egyéb, jel és kép továbbítását lehetővé tevő, fény- vagy hangjelzést adó, valamint egynél több csatornán átjelezni képes, belépési jogok automatizált kezelését biztosító elektronikus berendezések, műszaki megoldások összessége, amely a fizikai védelmet szolgálja;

9. *fizikai réteg:* az ISO/OSI referenciamodell legalsó rétege, amely biteket, bitsorozatokat továbbít

egymással kapcsolatban álló számítógépek közt, valamint biztosítja az ehhez szükséges mechanikai, funkcionális, elektronikus és eljárási eszközöket;

10. *fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fő részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai védelem, az élőerős védelem, a tápáramellátás, a sugárzott és vezetett zavarvédelem, a klimatizálás és a tűzvédelem;

11. *határon átnyúló fedezet:* olyan fedezet, amely a következő sajátosságok közül legalább egynek eleget tesz:

a) külföldi pénznemben nyilvántartott, kibocsátott eszköz,

b) külföldi jog fennhatósága alatt lévő eszköz,

c) kibocsátója külföldi jog fennhatósága alatt alapított vagy külföldi székhellyel rendelkezik;

12. *katasztrófaelhárítás:* krízishelyzetben a katasztrófa-helyreállítási tervben meghatározott akciótervek alapján elvégzett intézkedések összessége, amelyek végeredményeként a kritikus tevékenységek támogatására szolgáló informatikai alkalmazások és támogató erőforrások az ügyfelekkel kötött szerződésekben és az üzletszabályzatban vállalt mértékben újból rendelkezésre állnak, azzal, hogy amennyiben a krízishelyzetben a transzfer megbízások és egyéb üzenetek fogadása

a) folyamatos, úgy ide értendő a transzfer megbízások és egyéb üzenetek feldolgozása is,

b) szünetel, úgy ide értendő a rendkívüli esemény miatti, üzenetfogadásra vonatkozó szünet bekövetkeztét megelőzően érkező transzfer megbízások és egyéb üzenetek feldolgozása, amennyiben a pénzforgalom lebonyolításáról szóló MNB rendelet eltérően nem rendelkezik;

13. *katasztrófa-helyreállítási terv (DRP):* krízishelyzet esetén a kritikus tevékenységek támogatására szolgáló informatikai alkalmazások, támogató erőforrások lehető leggyorsabb visszaállítására, helyreállítására vonatkozó akciótervek összessége;

14. *kritikus tevékenység:* üzleti hatáselemzés alapján meghatározott, azon üzleti tevékenységek, szolgáltatások, amelyeket érintő rendkívüli esemény jelentős működési, pénzügyi, reputációs, jogi kockázatot okozna az üzleti folyamatban;

15. *krízishelyzet:* rendkívüli esemény nyomán kialakult, az együttműködő felek szokásos napi tevékenységétől eltérő eljárást igénylő helyzet;

16. *külső szolgáltató:* a rendszerüzemeltetőtől vagy a teljesítő féltől különböző szervezet, amely szerződéses keretek között nyújtott szolgáltatásával hozzájárul a fizetési rendszer zavartalan működéséhez;

17. *likviditás:* a fizetési rendszerben a transzfer megbízások teljesítésére fedezetül felhasználható eszközök összessége;

18. *logikai biztonság:* mindazon védelmi intézkedések összessége, amely a fizetési rendszer informatikai rendszereinek biztonságos működtetését megelőző és feltáró módon - kiemelten a biztonsági rendszerek működtetésével - felügyeli és ellenőrzi, és ennek érdekében szükség szerint beavatkozik;

19. *mélységi védelem:* a logikai biztonság területén a védelem rétegezésének stratégiája, amelynek keretében egyidejűleg több különböző módszerrel történik a védelmi intézkedések kialakítása;

20. *pénzügyi infrastruktúra:* a transzfer megbízások, értékpapírok, származtatott ügyletek vagy egyéb pénzügyi tranzakciók elszámolására, teljesítésére vagy nyilvántartására szolgáló, résztvevő intézmények közötti multilaterális rendszer, mely tartalmazza a rendszerüzemeltetőt is;

21. *rendkívüli esemény:* mindazon emberi magatartások, továbbá természeti vagy technikai eredetű események, amelyek a rendszerüzemeltető lényeges erőforrásainak, rendszereinek - e rendszerek összetevőinek, folyamatainak - hibáját, károsodását, működésük lassulását vagy megszűnését okozva fenyegetést jelenthetnek a rendszerüzemeltető által működtetett fizetési rendszer működésére nézve, továbbá olyan esemény, amelynek következtében a fizetési rendszer vagy a biztonsági rendszer informatikai környezetében tárolt információ bizalmassága, sértetlensége, hitelessége vagy rendelkezésre állása sérül;

22. *rendszerüzemeltető:* a fizetési rendszer működtetéséért, azaz a fizetési műveletek feldolgozásáért, elszámolásáért, valamint erre irányuló megállapodás esetén a fizetési műveletek teljesítéséért

polgári jogi felelősséggel tartozó szervezet;

23. *résztvevő:* a rendszerüzemeltető által működtetett fizetési rendszerhez csatlakozó intézmény, tekintet nélkül arra, hogy a fizetési rendszer működtetéséről szóló megállapodásban részes fél-e, ezen belül

a) közvetlen résztvevő: az az együttműködő fél, amely a saját és megbízói fizetési műveleteiből származó követelését és tartozását a teljesítő fél által vezetett teljesítési számláján a többi közvetlen résztvevő teljesítési számlájával vagy egy központi technikai számlával szemben rendezi,

b) közvetett résztvevő: az az intézmény, amely javára és terhére szóló fizetési műveletek a fizetési rendszerben közvetlen résztvevőként eljáró intézménynél vezetett fizetési számláján kerülnek teljesítésre;

24. *teljesértékű helyszín:* olyan helyiség, épület vagy épületrész, ahol a kritikus tevékenység nyújtásához szükséges infrastruktúra rendelkezésre áll, illetve a fizetési rendszer működtetésében részt vevő személyek dolgozhatnak, valamint amely rendkívüli esemény bekövetkezése esetén képes másik helyszín nélkül a teljes fizetési rendszert kiszolgálni;

25. *teljesítés:* a fizetési rendszer közvetlen résztvevői közötti tartozások és követelések kiegyenlítése a teljesítő fél által vezetett teljesítési számlákon;

26. *teljesítési számla:* a fizetési, illetve értékpapír-elszámolási rendszerekben történő teljesítés véglegességéről szóló törvényben (a továbbiakban: Tvt.) meghatározott teljesítési számla;

27. *teljesítő fél:* a teljesítést végző együttműködő fél, amely a közvetlen résztvevők teljesítési számlájának számlavezetőjeként végzi a teljesítést;

28. *transzfer megbízás:* a Tvt. szerinti transzfer megbízás, ideértve a pénzforgalmi szolgáltatás nyújtásáról szóló törvény szerinti fizetési megbízást, fizetési műveletet, valamint egy másik fizetési vagy értékpapír-elszámolási rendszer működtetője által benyújtott fizetésre szóló megbízást;

29. *újraindítás:* a rendkívüli eseményt követően a transzfer megbízások és egyéb üzenetek fogadásának ismételt biztosítása a katasztrófa-helyreállítási terv alapján azzal, hogy amennyiben a katasztrófaelhárítás alatt a transzfer megbízások és egyéb üzenetek fogadása

a) a 12. pont *a)* alpontja szerint teljesül, úgy az újraindítás egybeesik a katasztrófaelhárítással,

b) a 12. pont *b)* alpontja szerinti teljesül, az újraindítás a katasztrófaelhárítást követő tevékenység;

30. *üzenet:* a fizetési rendszerben a transzfer megbízásokat tartalmazó, illetve az együttműködő felek értesítésére, utasításaira, lekérdezéseire, illetve a fizetési rendszer technikai értesítésére szolgáló szabványos adathalmaz, információ;

31. *üzletmenet-folytonossági terv:* krízishelyzet esetén a kritikus tevékenység és a kapcsolódó üzleti folyamatok működését alternatív módon biztosító eljárásokat tartalmazó akciótervek összessége, rendszere, szükség szerint a katasztrófaelhárítás folyamatának kiegészítő eleme;

32. *védendő helyiség:* olyan helyiség, ahol a fizetési rendszer működtetését végző informatikai rendszer üzemel, továbbá minden olyan a fizetési rendszer működtetésével közvetlenül kapcsolatban lévő - a rendszerüzemeltető vagy a teljesítő fél által a titokvédelem szempontjából fontosnak minősített - helyiség, ahol üzleti vagy banktitkot, fizetési titkot és személyes adatokat tartalmazó iratokat, adathordozókat tárolnak, üzleti vagy banktitoknak vagy fizetési titoknak minősülő, illetve személyes adatokat dolgoznak fel vagy kezelnek.

2. A fizetési rendszer működtetésének általános feltételei

Az irányítási rendre vonatkozó követelmények

3. § (1) A rendszerüzemeltető olyan stratégiával rendelkezik, amely az általa működtetett fizetési rendszer biztonságos és hatékony működését alapvető célként kiemelten veszi figyelembe, továbbá támogatja a pénzügyi rendszer stabilitását, a nyílt és hatékony pénzügyi piacokat.

(2) A rendszerüzemeltető hatékony irányítási renddel rendelkezik, amelyre vonatkozó szabályzatok egyértelmű, egymástól elhatárolt felelősségi és elszámoltathatósági rendet határoznak meg. A

rendszerüzemeltető az irányítási rendre vonatkozó szabályzatait a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény (a továbbiakban: MNB tv.) 4. § (5) és (9) bekezdése szerinti feladatkörében eljáró MNB részére, valamint a rendszerüzemeltető tulajdonosai és a fizetési rendszer résztvevői számára elérhetővé teszi, és azok összefoglalóját - a (3) bekezdés *b)-d)* pontjában meghatározottak kivételével - honlapján közzéteszi.

(3) Az irányítási rendre vonatkozó szabályzatokban a rendszerüzemeltető az irányítási jogkörrel rendelkező vezető testületének felelősségi és feladatkörét egyértelműen meghatározza, amely - feltéve, hogy az nem a tulajdonos jogkörébe tartozik - kiterjed különösen

a) a fizetési rendszerre vonatkozó egyértelmű stratégiai célok meghatározására vonatkozó javaslattételre,

b) a fizetési rendszer működtetéséhez kapcsolódó döntéshozatali rend kialakítására, ideértve az irányítási jogkörrel rendelkező vezető testület tagjai közötti érdekellentét azonosításának és kezelésének módját is,

c) kritikus tevékenység irányításáért felelős legmagasabb szintű vezetők hatékony kiválasztásának, munkájuk nyomon követésének és amennyiben szükséges, munka alóli felmentésük rendjére, valamint

d) a kritikus tevékenység irányításáért felelős legmagasabb szintű vezetők vonatkozásában megfelelő javadalmazási irányelvek kialakítására, összhangban a bevált gyakorlattal és a hosszú távú eredményességre alapozva.

(4) Az irányítási rendre vonatkozó szabályzatokat az irányítási jogkörrel rendelkező vezető testület legalább évente egyszer áttekinti.

(5) A rendszerüzemeltető az irányítási rendre vonatkozó szabályzataiban egyértelműen és áttekinthetően meghatározza a kritikus tevékenység irányításáért felelős legmagasabb szintű vezetők felelősségi és feladatkörét, valamint beszámolási rendjét.

(6) A rendszerüzemeltető az irányítási rendre vonatkozó szabályzataiban úgy határozza meg a vezető állású személyek hatáskörét, hogy azok megfelelő felhatalmazással kísérjék figyelemmel

a) a rendszerüzemeltető tevékenységét, hogy az összhangban áll-e céljaival, stratégiájával és kockázatkezelési politikájával,

b) a belső kontroll funkciókat, hogy azok megfelelően tervezettek, működtetettek-e a rendszerüzemeltető (1) bekezdés szerinti céljainak támogatása érdekében,

c) a belső kontroll funkciókat és az ahhoz kapcsolódó eljárásokat, hogy azok rendszeres felülvizsgálatra és tesztelésre kerülnek-e megfelelően képzett és elégséges létszámú belső kontroll funkciókat ellátó szervezeti egységek által,

d) a kockázatkezelési folyamatot és

e) a kockázatkezelési keretrendszer és az üzletmenet-folytonossági tervek megfelelő működését.

(7) Az irányítási rendre vonatkozó szabályzatoknak biztosítaniuk kell, hogy az üzemeltetés, kockázatkezelés, megfelelőség biztosítás és belső ellenőrzés szervezetileg elkülönült legyen, megfelelő hatáskörrel, függetlenséggel és erőforrással rendelkezzen, valamint az irányítási jogkörrel rendelkező vezető testületnek rendszeresen beszámoljon.

(8) A rendszerüzemeltető az irányítási rendre vonatkozó szabályzataiba foglalt rendelkezésekkel biztosítja, hogy a fizetési rendszer technikai és funkcionális felépítésére, szabályaira, az (1) bekezdés szerinti stratégiájára, különösképpen az elszámolási és kiegyenlítési modellre, működési struktúrájára, az elszámolt és kiegyenlített termékek körére, a technológia és eljárások alkalmazására vonatkozó jelentős döntések előkészítése és a döntéshozatal során a fizetési rendszer együttműködő feleinek érdekei is figyelembevételre kerüljenek. Az irányítási rendre vonatkozó szabályzatok meghatározzák a nyilvános tájékoztatás rendjét.

Átfogó kockázatkezelési keretrendszer

4. § (1) A rendszerüzemeltető a fizetési rendszerben keletkező és viselt kockázatok átfogó és teljes

körű azonosítása, mérése, folyamatos nyomon követése, ellenőrizhetősége és kezelése céljából átfogó kockázatkezelési keretrendszert alakít ki és tart fenn, melyet az irányítási jogkörrel rendelkező vezető testület fogad el. A kockázatkezelési keretrendszert a rendszerüzemeltető rendszeresen felülvizsgálja.

Az átfogó kockázatkezelési keretrendszer

a) tartalmazza a rendszerüzemeltető kockázatkezelési politikáját és a megfelelő kockázatkezelési eszközöket magában foglaló kockázatkezelési rendszert,

b) biztosítja a kockázatkezelési rendszer folyamatos irányítását az irányítási jogkörrel rendelkező vezető testület számára,

c) kijelöli a kockázatvállaláshoz kapcsolódó felelősségi köröket, és biztosítja az e téren hozott döntésekért való elszámoltathatóságot,

d) rendelkezik a vész- és válsághelyzeti döntéshozatal rendjéről, valamint

e) meghatározza a belső kontroll funkciók kockázatkezelési rendszerrel kapcsolatos feladatköreit.

(2) A rendszerüzemeltető legalább évente egy alkalommal az átfogó kockázatkezelési keretrendszere alapján, a rendkívüli eseményekben realizálódó lehetséges kockázatok teljes körének felmérésén és elemzésén alapuló kockázatelemzést végez, amely tartalmazza

a) a fizetési rendszer szolgáltatásainak és az azokhoz tartozó folyamatoknak, ideértve a kritikus tevékenységeket is, a teljes körű felmérését,

b) a folyamatok prioritási sorrendbe helyezését, mely sorrend irányadó az üzletmenet-folytonossági tervezés során,

c) a folyamatokhoz kötődő lehetséges kockázati események körének teljes körű feltérképezését, valamint

d) a folyamatokhoz rendelt kockázati események bekövetkeztekor várható kár becslését, amennyiben ez lehetséges, a várható kár pénzösszegben való meghatározását (kockázati szintek).

(3) Az átfogó kockázatkezelési keretrendszer részeként a rendszerüzemeltető a (2) bekezdés *a)* pontjában meghatározottak alapján a kritikus tevékenységek rendelkezésre állását mutatószámokkal méri.

(4) A rendszerüzemeltető a kockázatelemzés részeként legalább évente egy alkalommal átfogó információbiztonsági kockázatelemzést készít, amely tartalmazza legalább

a) a potenciális fenyegetettségek és sérülékenységek bekövetkezési valószínűségének és hatásának teljes körű felmérését, így különösen a kockázatok folyamat szintű felmérésére vagy az információbiztonsági vagyonelem-leltár elemeire vonatkozóan,

b) a javaslatot az azonosított információbiztonsági kockázatok kezelésére.

(5) A rendszerüzemeltető oktatással, illetve tesztek előírásával és konzultáció biztosításával ösztönzi a résztvevőket - valamint amennyiben értelmezhető az ügyfelekre, akkor a résztvevők ügyfeleit - a kockázatok kezelésére és csökkentésére mindazon kockázat vonatkozásában, amelyek a résztvevők, illetve az ügyfelek tevékenysége következtében jelentkezhetnek a fizetési rendszerben és amelyek a fizetési rendszer működésének általuk viselt kockázatai.

(6) A rendszerüzemeltető azonosítja a fizetési rendszerben a kapcsolódó pénzügyi infrastruktúrákat, a forgalom tételszáma és értéke alapján a kritikus résztvevőket és potenciális hatásukat a többi résztvevőre és a fizetési rendszer egészére jelentős működési problémájuk esetén.

(7) A rendszerüzemeltető meghatározza, nyomon követi, és legalább évente felülvizsgálja a kölcsönös függőségek eredményeként a kritikus résztvevőktől, kapcsolódó pénzügyi infrastruktúráktól, illetve külső szolgáltatóktól származó, általa viselt, valamint más jogalanyokra gyakorolt jelentős kockázatokat. A rendszerüzemeltető az azonosított kockázati szintnek megfelelő és hatékony kockázatkezelési rendszert működtet.

Hitelkockázat kezelésére vonatkozó követelmények

5. § (1) A rendszerüzemeltető megfelelő és áttekinthető hitelkockázati keretrendszert alakít ki,

amely biztosítja a fizetési rendszerben az elszámolásból és teljesítésből származó hitelkockázati kitettség, illetve a résztvevők közötti hitelkockázati kitettség meghatározását, ennek keretében azonosítja a hitelkockázatot eredményező tevékenységeket és eseményeket.

(2) A rendszerüzemeltető, amennyiben a teljesítés módja alapján indokolt, a hitelkockázati kitettségek értékének nyomon követését minden munkanapon valós időben elvégzi.

(3) A rendszerüzemeltető a hitelkockázatok kezelésére megfelelő eszközöket és eljárásokat alkalmaz.

A fedezet és annak kezelésére vonatkozó követelmények

6. § (1) A rendszerüzemeltető a fedezet értékelésére és kezelésére vonatkozó olyan politikát és eljárásrendet alakít ki, illetve a teljesítő féllel kötött megállapodásban gondoskodik annak biztosításáról, hogy a teljesítő fél ezeket kialakítsa, amellyel a rendszerüzemeltető, illetve a teljesítő fél a jelen §-ban meghatározott kötelezettségeinek eleget tud tenni és nyomon tudja követni a fedezetként elfogadott minden egyes eszköz esetében azok hitelminőségét, piaci likviditását és árvolatilitását. A rendszerüzemeltető, illetve a teljesítő fél folyamatosan ellenőrzi és a fizetési rendszer kockázati kitettségére ható jelentős változás esetén, de legalább évente felülvizsgálja a fedezetek értékelésére és azok kezelésének követelményeire vonatkozó politikáját.

(2) A rendszerüzemeltető, illetve a teljesítő fél fedezetként csak a következő eszközöket fogadhatja el:

a) készpénz, valamint

b) alacsony hitel-, likviditási és piaci kockázattal rendelkező eszköz.

(3) A rendszerüzemeltető, illetve a teljesítő fél a fedezetek értékelésére és azok kezelésének követelményeire vonatkozó politikájában és eljárásrendjében objektív értékelési módszertan alapján értékeli, hogy a fedezetként elfogadott eszköz miként teljesíti a következő feltételeket:

a) alacsony hitelkockázatú kibocsátó bocsátja ki,

b) szabadon átruházható bármely korlátozás, illetve harmadik fél jóváhagyása nélkül,

c) olyan pénznemben denominált, amelynek kockázata kezelhető a rendszerüzemeltető által,

d) rendszeresen frissülő és közzétett, megbízható árral rendelkezik,

e) nincs kitéve jelentős rossz irányú kockázatnak, valamint

f) nem a fedezetet nyújtó résztvevő vagy a résztvevő kapcsolt vállalkozása bocsátja ki.

(4) A rendszerüzemeltető, illetve a teljesítő fél az objektív értékelési módszertanát - beleértve a fedezetként elfogadott eszközök befogadási értékének meghatározását is - rendkívüli piaci viszonyokat is szimuláló forgatókönyvek alapján legalább évente teszteli, és a tesztek eredménye alapján felülvizsgálja.

(5) A rendszerüzemeltető, illetve a teljesítő fél olyan kockázatmérséklő befogadási értéket határoz meg és alkalmaz, amely rendkívüli piaci mozgások esetén is megfelelő mértékű fedezeti szintet biztosít, és az érték meghatározásának módszerét olyan munkavállaló hagyja jóvá, aki nem vett részt a módszertan kidolgozásában.

(6) A rendszerüzemeltető, illetve a teljesítő fél olyan intézkedéseket határoz meg, amellyel elkerülhető, hogy a fedezetként elfogadott eszközök esetében olyan jelentős koncentráció jöjjön létre, amivel jelentős negatív árhatás nélkül nem lehet gyorsan értékesíteni ezeket az eszközöket.

(7) Amennyiben a rendszerüzemeltető, illetve a teljesítő fél elfogad határon átnyúló fedezetet, akkor az annak használatához kapcsolódó kockázatokat azonosítja és csökkenti, valamint biztosítja, hogy a határon átnyúló fedezet szükség esetén felhasználható legyen.

(8) A rendszerüzemeltető, illetve a teljesítő fél a fedezet értékelésére és kezelésére vonatkozó politikának megfelelő hatékony és rugalmasan változtatható fedezetkezelési eljárásrendet alakít ki és tart fenn, amelyet a fizetési rendszer kockázati kitettségére ható jelentős változás esetén, de legalább évente felülvizsgál.

A likviditási kockázat kezelésére vonatkozó követelmények

7. § (1) A rendszerüzemeltető átfogó likviditási kockázat kezelésére vonatkozó keretrendszerrel rendelkezik, - illetve a teljesítő féllel kötött megállapodásban biztosítja, hogy a teljesítő fél átfogó likviditási kockázat kezelésére vonatkozó keretrendszerrel rendelkezzen - ahhoz, hogy a rendszerüzemeltető, illetve a teljesítő fél az együttműködő felekhez köthető likviditási kockázatot értékelje és kezelje.

(2) A rendszerüzemeltető, illetve a teljesítő fél a fizetési forgalom, illetve a fizetési forgalom lebonyolítására rendelkezésre álló napközbeni likviditás folyamatos és kellő időben történő azonosítására, mérésére, nyomon követésére működési (technikai) és analitikai (nyilvántartási) eszközzel rendelkezik.

Pénzben történő teljesítés

8. § (1) A rendszerüzemeltető biztosítja, hogy - a (2)-(4) bekezdésben foglaltak kivételével - a teljesítés jegybankpénzben történjen.

(2) Amennyiben a jegybankpénzben történő teljesítés nem lehetséges, akkor a rendszerüzemeltető a teljesítést olyan eszközben biztosítja, amely nem vagy kismértékben von maga után hitel- és likviditási kockázatot.

(3) Amennyiben a rendszerüzemeltető jár el teljesítő félként, saját hitel- és likviditási kockázatát nyomon követi, kezeli és csökkenti. Amennyiben nem a rendszerüzemeltető jár el teljesítő félként, a rendszerüzemeltető és a teljesítő fél egymással e tárgyban megállapodást köt, amely tartalmazza

a) a teljesítés időpontját,

b) a teljesítés véglegességének és visszavonhatatlanságának időpontját, valamint

c) a teljesítő fél kötelezettségét annak biztosítására, hogy a jóváírt pénzösszeg a lehető legrövidebb időn belül átutalható legyen, de legkésőbb a munkanap végén.

(4) Amennyiben teljesítő félként hitelintézet jár el, a rendszerüzemeltető nyomon követi, kezeli és korlátozza a teljesítő félként eljáró hitelintézetre vonatkozó hitel- és likviditási kockázatát. A rendszerüzemeltető a teljesítő félként eljáró hitelintézettel szemben a hitelképességére, tőkeellátottságára, likviditáshoz való hozzáférésére és működési megbízhatóságára vonatkozóan szigorú feltételeket támaszt, és azok betartását figyelemmel kíséri. A rendszerüzemeltető a teljesítő félként eljáró hitelintézettel szembeni hitel- és likviditási kockázat koncentrációjának lehetőségét is nyomon követi és kezeli.

A résztvevői nemteljesítések kezeléséhez kapcsolódó követelmények

9. § (1) A rendszerüzemeltető a teljesítő féllel, valamint az MNB tv. 4. § (9) bekezdése szerinti feladatkörében eljáró MNB-vel kötött együttműködési megállapodásban rögzíti a résztvevői nemteljesítéshez kapcsolódó eljárásokat.

(2) A rendszerüzemeltető a résztvevői nemteljesítéshez kapcsolódó eljárásokat az érintett felek bevonásával teszteli, és a tesztek eredménye alapján az eljárások felülvizsgálatát rendszeresen, de legalább évente egyszer elvégzi az eljárások hatékonyságának biztosítása érdekében.

Az általános üzleti kockázat kezelése

10. § (1) A rendszerüzemeltető szilárd irányítási és ellenőrzési rendszert alakít ki az általános üzleti kockázat azonosítására, folyamatos nyomon követésére és kezelésére, ideértve az üzleti stratégia rossz kivitelezéséből, a reputáció romlásából, a negatív pénzáramlásból vagy a nem várt, illetve túlzóan nagy működési költségekből eredő veszteségek kezelését is.

(2) A rendszerüzemeltető az általános üzleti kockázatok kezelésére vonatkozó, megvalósítható

tervvel rendelkezik.

(3) A rendszerüzemeltető általános üzleti tevékenységei és a kritikus tevékenységek folytatásához szükséges időkeret alapján határozza meg az általános üzleti kockázatok kezeléséhez szükséges eszközértéket, mely érték legalább megegyezik a rendszerüzemeltető adott időszakot megelőző 3 naptári hónap működési költségeinek összegével.

(4) A rendszerüzemeltető az általános üzleti kockázatok kezelésére szükséges eszközérték fedezeteként rendelkezik tőkéből fedezett nettó likvid eszközzel (mint törzsrészvény, tartalékok), amely megfelelően likvid, megfelelő minőségű és a kellő időben felhasználható, és amelyet a rendszerüzemeltető a napi működését biztosító eszközöktől elkülönítve nyilvántart, annak érdekében, hogy az általános üzleti veszteség előfordulása esetén is folytatni tudja működését. Ezek az eszközök fedezetül szolgálnak a résztvevői nemteljesítés fedezetére, illetve az 5. §-ban és a 7. §-ban meghatározott kockázatok fedezetére is.

(5) A rendszerüzemeltető megvalósítható, további tőke bevonását lehetővé tévő tervvel rendelkezik arra az esetre, ha a jegyzett tőkéje az általános üzleti kockázatok kezelésére vonatkozó terv megvalósításához szükséges eszközérték összegét megközelítené vagy az alá esne.

A letétkezelői és a befektetési kockázat kezelése

11. § (1) A rendszerüzemeltető a saját pénzeszközeit hitelintézetnél tartja.

(2) A rendszerüzemeltető a résztvevők által rendelkezésére bocsátott pénzeszközöket hitelintézetnél (a továbbiakban: letétkezelő) tartja letéti számlán.

(3) A rendszerüzemeltető azonnali hozzáféréssel rendelkezik a letéti számlán elhelyezett pénzeszközökhöz.

(4) A rendszerüzemeltető értékeli kockázati kitettségét a letétkezelővel szemben, ennek során mindenféle típusú kapcsolatát, a letétkezelő által nyújtott szolgáltatások teljes körét figyelembe veszi adott letétkezelő vonatkozásában.

12. § (1) A rendszerüzemeltető befektetési stratégiája összhangban áll a kockázatkezelési stratégiájával.

(2) A rendszerüzemeltető a befektetési stratégiáját legalább évente felülvizsgálja.

(3) A rendszerüzemeltető az eszközeit magas minősítéssel rendelkező kötelezettek által biztosított, vagy velük szembeni igényen alapuló eszközbe vagy alacsony hitel-, piaci és likviditási kockázatot hordozó pénzügyi eszközökbe fekteti be.

A résztvevői szintekhez kapcsolódó követelmények

13. § (1) A rendszerüzemeltető biztosítja, hogy a szabályzatai, eljárásrendje, szerződései lehetővé tegyék a közvetett résztvevőkről szóló információk összegyűjtését, annak érdekében, hogy a rendszerüzemeltető képes legyen a résztvevői szintekből származó jelentős kockázatokat azonosítani, nyomon követni és kezelni.

(2) A közvetett résztvevőkről szóló információk minimum a következőkre terjednek ki egy adott időszakra, de legalább egy évre vonatkozóan:

a) a közvetett résztvevők száma,

b) az egyes közvetlen résztvevők esetében a saját és a rajtuk keresztül csatlakozó közvetett résztvevők forgalmának (érték és tételszám) részaránya a rendszerszintű forgalomhoz viszonyítva,

c) az egyes közvetett résztvevők által lebonyolított forgalom értéke és tételszáma, és

d) a *c)* pontban meghatározott forgalom (érték és tételszám) részaránya azon közvetlen résztvevő forgalmához viszonyítva, amelyen keresztül csatlakozik a fizetési rendszerhez.

(3) A rendszerüzemeltető a vonatkozó kockázatok kezelése érdekében a (2) bekezdésben meghatározott információk alapján azonosítja

a) a közvetlen és közvetett résztvevők közötti jelentős mértékű függőségi viszonyokat, melyek

kihathatnak a fizetési rendszer működésére,

b) a közvetett résztvevőket, akik jelentős kockázatot jelentenek a fizetési rendszerre, és

c) azon közvetlen résztvevőket, akiken keresztül ezen közvetett résztvevők a fizetési rendszerhez csatlakoznak.

(4) A rendszerüzemeltető legalább évente felméri a résztvevői szintekből származó kockázatokat, és amennyiben szükséges, azokat a 4. § (2) bekezdése szerinti kockázatelemzés keretében megfelelően kezeli.

3. A fizetési rendszer működtetésének tárgyi, technikai feltételei

14. § A fizetési rendszer nemzetközileg elfogadott kommunikációs eljárásokat, csatornákat és szabványokat használ, vagy saját eljárásait és szabványait ezekhez igazítja.

15. § (1) A rendszerüzemeltető legalább két teljesértékű helyszínnel rendelkezik.

(2) A rendszerüzemeltető irányítási jogkörrel rendelkező vezető testülete a 4. § (2) bekezdésében meghatározott kockázatelemzés eredményeinek figyelembevételével dönt a teljesértékű helyszín földrajzi helyéről, felszereltségéről és készültségi fokáról.

(3) A teljesértékű helyszín felszereltsége és készültsége, valamint a részleges és teljes áttelepülés eljárásrendje oly módon biztosítja a 26. § (5) bekezdésében meghatározott katasztrófaelhárítási és újraindítási idők teljesülését, hogy a rendszerüzemeltető a részleges vagy teljes áttelepülés során a fizetési rendszer működtetésével kapcsolatban vállalt minden kötelezettségét határidőre teljesíteni tudja.

(4) A rendszerüzemeltető a teljesértékű helyszín vonatkozásában csak olyan épületben vagy épületrészben működhet,

a) amely a rendszerüzemeltető saját tulajdonában áll, vagy

b) amelyet a rendszerüzemeltető határozatlan időtartamú, a bérlő javára legalább egyéves felmondási időt biztosító szerződéssel kizárólagosan bérel.

(5) A fizetési rendszer működtetését támogató informatikai rendszerek, valamint a fizetési rendszer működésének zavartalanságát biztosító egyéb eszközök folyamatos energiaellátása érdekében a rendszerüzemeltető tartalék energiaforrással és szünetmentes tápellátással rendelkezik, és ennek rendeltetésszerű működéséről legalább 12 havonta jegyzőkönyv felvétele mellett meggyőződik. A fizetési rendszer működtetését támogató egyéb energia- és erőforrások, valamint nyersanyagok tekintetében a rendszerüzemeltető olyan alternatív forrásokat határoz meg, amelyek az elsődleges források kiesése esetén biztosítják a folyamatos működést. A rendszerüzemeltető védi a fizetési rendszert támogató informatikai rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben, lehetőséget biztosít az informatikai rendszer áramellátásának kikapcsolására vészhelyzetben, gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről és a jogosulatlan vészkikapcsolás megakadályozásáról.

(6) A fizetési rendszer működtetéséhez az együttműködő felek között szükséges üzenetáramlás folyamatossága érdekében a rendszerüzemeltető az együttműködő felek és a rendszerüzemeltető teljesértékű helyszínei között legalább kettő egyenrangú információközvetítő fizikai réteggel rendelkezik, amelyekkel kapcsolatban elvárás, hogy

a) egymástól elkülönülten lépjenek be a teljes körű helyszínre,

b) a rendszerüzemeltető törekedjen arra, hogy eltérő külső szolgáltatók biztosítsák.

(7) Amennyiben a fizetési rendszer lehetővé teszi, a rendszerüzemeltető az üzletmenet-folytonosság biztosítása érdekében legalább két független üzenetközvetítő csatornával rendelkezik.

(8) A rendszerüzemeltető a fizetési rendszer teljesértékű helyszínének feldolgozókapacitását oly módon alakítja ki, hogy az az alkalmazott technológia függvényében meghatározott kapacitástöbblettel növelve biztosítsa a transzfer megbízások fizetési rendszer szabályaiban meghatározott határidőn belül történő feldolgozását. A rendszerüzemeltető folyamatos kapacitásmenedzsmenttel, eszköz- és szabályrendszerrel, továbbá az üzleti elvárásokat biztosító, skálázható kapacitással

rendelkezik. Az alkalmazott architektúramegoldásoknak támogatniuk kell egy jövőbeli, reálisan prognosztizálható kapacitásigényekre történő átalakítás képességét is, amely egy rendkívüli piaci helyzetben esetlegesen megnövekedett tételszámot is képes kezelni a vállalt szolgáltatási szint teljesítésével együtt. A rendszerüzemeltető a fizetési rendszer teljesértékű helyszíne feldolgozókapacitásának megfelelőségét az informatikai környezet jelentős változásával járó minden módosítás esetén ellenőrzi.

16. § (1) A rendszerüzemeltető a fizetési rendszer működtetése tevékenységhez kapcsolódóan igénybe vett külső szolgáltató által nyújtott szolgáltatásra a szolgáltatási szintet megfelelő részletességgel szabályozó szerződést köt.

(2) A külső szolgáltatóval kötött szerződés tartalmazza

a) a szolgáltatás leírását,

b) a szolgáltatás ellátásához használt eszközök és megoldások körét,

c) a külső szolgáltató és a rendszerüzemeltető közötti kommunikációs módok leírását,

d) a rendszerüzemeltető elvárásait és a teljesítés ellenőrzésének szabályait,

e) a rendkívüli események besorolását és a külső szolgáltató által vállalt kiszállási és hibajavítási határidőket,

f) a felmerülő hibák javítása során a külső szolgáltató és a rendszerüzemeltető közötti munkamegosztás rendjét és a felelősségi határok kijelölését és a kapcsolattartók neveit, elérhetőségeit,

g) a külső szolgáltató által nyújtott eszköz vagy szolgáltatás kiváltására elegendő időt biztosító, egységesen mindkét fél részéről alkalmazható felmondási időt,

h) a fizetési rendszer működését befolyásoló külső technológiai változások követésének rendjét, és

i) egyedileg megtárgyalt szerződés esetén a rendszerüzemeltetőnek a külső szolgáltató vizsgálatára és ellenőrzésére vonatkozó korlátlan jogát, a külső szolgáltató mindezekhez való kifejezett hozzájárulását, a külső szolgáltató együttműködési kötelezettségét.

(3) A rendszerüzemeltető a külső szolgáltatóval olyan tartalmú szerződést köt, amely biztosítja a 26. § (5) bekezdésében foglalt katasztrófaelhárítási és újraindítási határidők teljesülését.

4. A fizetési rendszer működtetésének általános biztonsági feltételei

Szervezeti feltételek

17. § (1) A rendszerüzemeltető fizikai biztonsági szervezetet, valamint logikai biztonsági szervezetet működtet, amelyek nem lehetnek részei olyan szervezeti egységnek, amely felett felügyeleti vagy ellenőrzési feladatokat látnak el.

(2) A fizikai, illetve a logikai biztonsági szervezet ellátja a biztonsági tevékenységekkel kapcsolatos feladatokat így különösen

a) végzi, szervezi és felügyeli a felelősségi körébe tartozó rendkívüli esemény esetén követendő munkavállalói magatartására vonatkozó oktatást,

b) elemzéseket végez, és javaslatokat tesz a megfelelő védelmi intézkedésekre és a biztonsággal összefüggő szabályokra,

c) felelős a biztonságpolitika és a biztonsági szabályzat szakmai tartalmáért, aktualizálásáért,

d) humán és technikai eszközökkel folyamatosan biztosítja a rendkívüli események bekövetkezésének megelőzését, elkerülését,

e) ellenőrzi a biztonsági előírások végrehajtását,

f) hatékonyan beavatkozik a felelősségi körébe tartozó rendkívüli esemény bekövetkezésekor,

g) rendszeresen tesztek segítségével ellenőrzi a logikai és fizikai biztonság szintjét és azok megfelelőségét.

(3) A logikai biztonsági szervezet a (2) bekezdésben meghatározottakon túl legalább a következő feladatokat végzi:

a) ellátja a biztonsági rendszerek, így különösen tűzfalak, behatolásdetektálók, publikus kulcsú infrastruktúra felügyeletét és kontrollját,

b) rendszeresen kiértékeli, elemzi a logikai biztonsági feltételek megvalósulását,

c) tervezési feladatokat lát el, különösen a biztonsági architektúra megtervezését.

(4) Az (1) bekezdésben meghatározott két biztonsági szervezet működése ugyanazon szervezeti egységen belül is megvalósulhat. Ebben az esetben a szervezeti egység vezetője az lehet, aki megfelel mind az (5), mind a (6) bekezdésben foglalt követelményeknek.

(5) A rendszerüzemeltető a fizikai biztonsági tevékenység irányítására olyan személyt alkalmaz, aki

a) a rendszerüzemeltetővel munkaviszonyban áll,

b) rendőrtiszti vagy katonai főiskolai vagy egyetemi végzettséggel, egyéb egyetemi vagy főiskolai és felső középfokú biztonsági szakképesítést nyújtó végzettséggel, valamint

c) legalább hároméves, biztonsági, védelmi területen szerzett gyakorlattal rendelkezik.

(6) A rendszerüzemeltető a logikai biztonsági tevékenység irányítására olyan személyt alkalmaz, aki

a) a rendszerüzemeltetővel munkaviszonyban áll,

b) információ-technológiai főiskolai vagy egyetemi végzettséggel, egyéb egyetemi vagy főiskolai és felsőközépfokú informatikai biztonsági szakképesítést nyújtó végzettséggel, valamint

c) legalább hároméves, informatikai biztonsági területen szerzett gyakorlattal rendelkezik.

(7) A fizikai biztonsági szervezet, valamint a logikai biztonsági szervezet vezetője a felelősségi körébe tartozó jelentős rendkívüli esemény esetén, de legalább évente egy alkalommal beszámol az irányítási jogkörrel rendelkező vezető testületnek.

(8) A rendszerüzemeltető olyan összeférhetetlenségi szabályokat alkot, amelyek biztosítják a biztonsági szervezet jelen alcímben foglalt feladatainak ellátását.

A fizikai és logikai biztonságra vonatkozó szabályzatok

18. § A rendszerüzemeltető a fizikai és a logikai biztonsággal kapcsolatos minden információt, tényt, megoldást és adatot, ideértve a biztonság céljából megteremtett tárgyi, technikai, logikai feltételeket és ezek műszaki dokumentumait is - törvény eltérő rendelkezése hiányában - üzleti titokként kezel.

19. § (1) A fizetési rendszer biztonságos működtetése érdekében a rendszerüzemeltető meghatározza a fizikai és a logikai biztonságra vonatkozó biztonságpolitikáját, és a fizikai és a logikai biztonság feltételeire vonatkozó elveket.

(2) A rendszerüzemeltető a biztonságpolitikája alapján elkészített, a biztonsági kockázatokkal és azok változásaival összhangban lévő, részletes védelmi intézkedéseket tartalmazó fizikai és logikai biztonsági szabályzatokkal rendelkezik.

(3) A fizikai biztonsági szabályzat tartalmazza

a) a biztonsági szervezet és a biztonságért felelős személy feladatait, hatáskörét,

b) a biztonság tárgyi feltételeinek (a továbbiakban: fizikai biztonsági feltétel) megvalósításához szükséges eszközöket, eljárásokat, technikát, az alkalmazandó műszaki specifikáció (ajánlás, szabvány, illetve műszaki engedély) feltüntetésével együtt, és a védelem formái szerinti csoportosításban,

c) azon épületeket (épületrészeket), ahol a védendő helyiségek elhelyezkednek,

d) a védendő helyiségek körét,

e) a rendkívüli események kezelésének általános és speciális szabályait,

f) a munkavállalók számára meghatározott, a biztonsági szabályok betartására vonatkozó általános és speciális felelősségi rendet,

g) a munkavállalókra vonatkozó személyi védelmi intézkedéseket, kiemelve a fokozott veszélynek kitett munkakörök (személyek) védelmét,

h) a munkavállalók biztonsági oktatásának rendjét,

i) a fizikai biztonsági ellenőrzés módszertanának leírását, az intézkedések és a szankcionálás rendjét, a módszertanok fejlődésének követési rendjét, valamint

j) a kiszervezett tevékenységekre vonatkozó fizikai biztonsági feltételeket, és e feltételek teljesülésének a rendszerüzemeltető által a kiszervezett tevékenységet végző külső szolgáltatóknál történő ellenőrzése során a fizikai biztonsági szervezet bevonására vonatkozó szabályt.

(4) A logikai biztonsági szabályzat tartalmazza

a) a rendszerüzemeltető logikai biztonságának kialakításához használt módszertan megnevezését,

b) a fizetési rendszer logikai felépítésének, fizikai kiterjedésének, a fizetési rendszer kapcsolatainak leírását,

c) a védendő adatok és informatikai erőforrások körét,

d) a fizetési rendszert érő lehetséges fenyegetéseket és ezek mindegyikének megelőzésére vonatkozó biztonsági követelményeket,

e) a logikai biztonság elemeit,

f) a logikai biztonsági megoldások fejlődésének követési rendjét,

g) a fizetési rendszer fejlesztésének és használatbavételének logikai biztonsági előírásait,

h) a fizetési rendszer működtetésére vonatkozó logikai biztonsági elvárásokat,

i) a fizetési rendszerrel kapcsolatos informatikai tevékenységekre vonatkozó ismereteket, szerepköröket, felelősségeket, jogosultságokat,

j) a fizetési rendszer működtetésében részt vevő valamennyi személy számonkérhetőségének módját és a sértetlenségét biztosító eljárásokat,

k) a logikai biztonsági ellenőrzés módszertanának leírását, az intézkedések és a szankcionálás rendjét, a módszertanok fejlődésének követési rendjét,

l) a kiszervezett tevékenységekre vonatkozó logikai biztonsági feltételeket és e feltételek teljesülésének a rendszerüzemeltető által, a kiszervezett tevékenységet végző külső szolgáltatóknál történő ellenőrzése során a logikai biztonsági szervezet bevonására vonatkozó szabályt és

m) a maradék kockázatoknak a rendszerüzemeltető irányítási jogkörrel rendelkező vezető testülete általi megismertetésének és jóváhagyásának rendszerét.

Fizikai biztonsági feltételek

20. § A rendszerüzemeltető a fizikai biztonsági feltételeket a tevékenységéhez kapcsolódó biztonsági kockázatok felmérése alapján, azokkal arányos módon és a vagyonbiztosításhoz szükséges követelmények figyelembevételével teremti meg.

21. § (1) A rendszerüzemeltető a biztonsági szabályzatában foglaltak alapján - a (2) bekezdésben foglaltak figyelembevételével - gondoskodik az elhelyezésére szolgáló épület (épületrész) és védendő helyiségek mechanikai-fizikai védelméről.

(2) A mechanikai-fizikai védelem feltételeinek kialakításakor, működtetésekor a jogszabályokban foglalt kötelezettségek mellett, figyelembe veszi és kockázatarányosan alkalmazza a Magyar Biztosítók Szövetsége (a továbbiakban: MABISZ) „Betöréses lopás- és rablásbiztosítás technikai feltételei” című ajánlásában foglaltakat.

(3) Elektronikus vagyonvédelmi rendszereket csak

a) a biztonsági szervezet vezetője vagy a rendszerüzemeltető szervezeti és működési szabályzatában meghatározott más személy által jóváhagyott terv alapján lehet telepíteni, és

b) a külön jogszabályban előírt szakirányú végzettséggel rendelkező személy tervezhet, telepíthet és tarthat karban.

(4) A rendszerüzemeltető biztosítja, hogy az elektronikus vagyonvédelmi rendszerek programozásához és a kezelői jogosultság kiadásához szükséges kódok a biztonsági szervezet vezetőjénél az általuk írásban felhatalmazott személynél vagy a rendszerüzemeltető szervezeti és működési szabályzatában meghatározott személynél, a biztonságos őrzés és a hozzáférési jogosultság

szabályozása mellett rendelkezésre álljanak.

(5) A rendszerüzemeltető gondoskodik automatikus távjelzés továbbítására alkalmas összeköttetés kiépítéséről és folyamatos működtetéséről az elektronikus vagyonvédelmi rendszerek és a 24 órás őrszolgálat által felügyelt és kezelt őrzésvédelmi központ vagy valamely távfelügyeleti szolgáltatást nyújtó vagyonvédelmi társaság fogadó központja között.

22. § (1) A rendszerüzemeltető biztosítja, hogy a fizetési rendszer működését támogató informatikai rendszerek elhelyezésére szolgáló helyiségek rendelkeznek

a) az ott elhelyezett számítástechnikai berendezések számára optimális hőmérsékletet biztosítani képes klímaberendezéssel,

b) tűzjelző berendezéssel,

c) a számítástechnikai berendezéseket nem károsító tűzoltási technológiával,

d) nedvességdetektáló berendezéssel,

e) víz- és más, csővezetéken szállított anyag okozta kár elleni védelemmel, továbbá

f) a hőmérséklet és a páratartalom megfelelő szinten tartását mérni képes környezetfelügyeleti rendszerrel.

(2) A rendszerüzemeltető gondoskodik arról, hogy az (1) bekezdés *b)*, *d)* és *f)* pontjában nevesített eszközök által adott figyelmeztető és hibajelzések legalább kettő, egymástól független értesítési csatornán keresztül eljussanak a fizetési rendszer működését felügyelő személyzethez.

23. § (1) A mechanikai-fizikai és az elektronikai védelem kialakítására a rendszerüzemeltető az Európai Unióban elfogadott minősítő szervezet vagy a MABISZ által kiadott, a biztonságtechnikai termék megfelelőségére vonatkozó ajánlással rendelkező eszközt alkalmaz.

(2) A rendszerüzemeltető gondoskodik a kizárólagos használatában lévő épületben vagy épületrészben üzemelő védendő helyiség védelmi rendszerbe történő beillesztéséről.

(3) A védendő helyiségek körére a rendszerüzemeltető a kockázatokkal arányos védelmet biztosító beléptető rendszerrel rendelkezik, amely biztosítja a személyek mozgásának visszakereshetőségét és egyértelmű azonosítását, ellenőrizhetőségét.

(4) A rendszerüzemeltető

a) a működését biztosító, a napi teendők ellátásához már nem szükséges iratokat, adathordozókat (számítógépes programok biztonsági másolata, archivált adatok, biztonsági mentések stb.) zárható és legalább 30 perces tűzállóságú elkülönített helyiségben vagy MABISZ minősítésű 30 perces tűzállóságú páncélszekrényben tárolja, és

b) az iratok és adathordozók másodpéldányát (másolatát) zárható és legalább 30 perces tűzállóságú, az *a)* pontban meghatározottól különböző, elkülönített helyiségben őrzi.

(5) A rendszerüzemeltető iratkezelési szabályzatban határozza meg azoknak az iratoknak és adathordozóknak a körét, amelyek tárolásáról és őrzéséről a (4) bekezdésben foglaltak szerint gondoskodik.

(6) A rendszerüzemeltető az elhelyezésére szolgáló épületre (épületrészre) vonatkozóan 24 órás őrszolgálatot biztosít, kivéve, ha a rendszerüzemeltető által stratégiai fontosságúnak minősített épületrész olyan épületben található, amely épület tulajdonosa vagy üzemeltetője az egész épületre vonatkozóan az e rendeletben foglaltaknak megfelelően biztosítja az őrszolgálatot.

(7) A rendszerüzemeltető az őrszolgálatot ellátó személy szolgálati helyét a helyi adottságok és a rendszerüzemeltető biztonságpolitikája alapján határozza meg. A rendszerüzemeltető gondoskodik arról, hogy az őrszolgálatot ellátó személy szükség esetén a rendkívüli helyzet elhárítása céljából a hatóságot vagy külső szolgáltatót távjelzéssel vagy távközlési vonalon keresztül vagy más alkalmas módon haladéktalanul értesíthesse.

Logikai biztonsági feltételek

24. § (1) A rendszerüzemeltető a fizetési forgalom lebonyolításának folyamatai tekintetében biztosítja a folyamatot alkotó egyes elemi események egyértelmű és visszakereshető azonosítását,

valamint - amennyiben ezek nem automatizált módon történtek meg - az elemi események személyekhez kötését.

(2) A rendszerüzemeltető biztosítja az együttműködő felek közötti üzenetáramlás letagadhatatlanságát minden üzenet tekintetében.

(3) A rendszerüzemeltető úgy alakítja ki a fizetési rendszer működési rendjét, hogy az az egyes, emberi közreműködést igénylő elemi események végrehajtásakor biztosítsa az emberi beavatkozásból fakadó esetleges hibák megelőzését segítő, folyamatba épített kontrollt.

(4) A rendszerüzemeltető folyamatosan naprakész felhasználó- és jogosultság-nyilvántartással rendelkezik.

(5) A rendszerüzemeltető megelőző, feltáró és beavatkozást lehetővé tevő módszerekkel biztosítja a fizetési rendszer személyekre, folyamatokra és a technológiára is kiterjedő mélységi védelem megközelítésű, kockázati alapú, többszintű rendszerfelügyeletének kiépítését és annak folyamatos működtetését.

(6) A rendszerüzemeltető biztosítja, hogy az informatikai környezetet és a logikai biztonsági intézkedéseket és megoldásokat befolyásoló változások a rendszerüzemeltető változáskezelési folyamatának részét képezik, továbbá biztosítja a változások megfelelő előkészítését, tervezését, tesztelését, dokumentálását és engedélyezését.

(7) A rendszerüzemeltető informatikai környezete csak akkor módosítható, ha a tervezett változtatás végrehajtásának kockázataival arányos, megfelelő időtartamú és tartalmú tesztelés alapján egyértelműen megállapítható, hogy a változás élesítése a fizetési rendszer működésében zavart nem okozhat. A rendszerüzemeltető a tesztelés során a tervezett változtatás végrehajtásának kockázataival arányosan gondoskodik

a) a funkciótesztek, ideértve az általános üzleti és szélsőérték funkcionális teszteket,

b) a biztonsági tesztek,

c) az informatikai funkciótesztek, úgy mint telepítési, részleges és teljes áttelepülési és rendszervisszaállítási tesztek és

d) a teljesítménytesztek

elvégzéséről. A rendszerüzemeltető a tesztelésbe a változtatás jellegétől függően bevonja az érintett együttműködő feleket és az érintett külső szolgáltatókat.

(8) A rendszerüzemeltető részletes nyilvántartást vezet a fizetési rendszer működése során bekövetkezett rendkívüli eseményekről, azok hatásáról (ezen belül külön részletezve a résztvevőkre gyakorolt hatást), a rendkívüli esemény okáról, a hiba elhárításának menetéről és a hiba jövőbeni előfordulását megelőző intézkedésekről. A nyilvántartás a rendkívüli eseményre vonatkozó információt az esemény bekövetkeztét követő 5 évig tartalmazza.

(9) A rendszerüzemeltető a logikai biztonsággal kapcsolatos szabályzatait, illetve a vonatkozó infrastruktúrát rendszeresen belső, illetve külső auditnak veti alá. A külső auditot legalább háromévente egy független, megfelelő szakértelemmel bíró személlyel vagy szolgáltatóval kell elvégeztetni.

(10) A rendszerüzemeltető biztosítja, hogy a biztonsági rendszerben elérhető és ezekhez kapcsolódó adatokról készített biztonsági mentések titkosítást követően kerüljenek tárolásra, valamint a logikai biztonsági tevékenységet irányító személy jóváhagyását követően legyenek hozzáférhetőek.

25. § (1) A rendszerüzemeltető hatékony kiberbiztonsági keretrendszerrel rendelkezik annak érdekében, hogy a kiberkockázatot kezelje.

(2) A rendszerüzemeltető azonosítja a kiberkockázattal érintett kritikus tevékenységeket és azokat támogató eszközöket. A rendszerüzemeltető megfelelő intézkedéseket hoz annak érdekében, hogy a kibertámadásokkal szemben védje azokat, illetve a kibertámadást felderítse, az esemény észlelésekor az érintett feleket haladéktalanul tájékoztassa, a kibertámadást elhárítsa és azt követően helyreállítsa a kritikus tevékenységeket és azokat támogató eszközök működését, valamint ezen intézkedéseket rendszeresen teszteli.

(3) A rendszerüzemeltető biztosítja a kiberfenyegetettséggel szembeni tudatosság megfelelő

szintjét.

(4) Annak érdekében, hogy a kiberkockázatban bekövetkező, jellemzően gyors változásokhoz időben alkalmazkodni tudjon, a rendszerüzemeltető biztosítja, hogy munkavállalói folyamatos tanulással és fejlődéssel a szükséges kiberbiztonságikeretrendszer-módosításokat időben elvégezzék.

5. A fizetési rendszer működtetésének üzletmenet-folytonossági és katasztrófaelhárítási feltételei

26. § (1) A rendszerüzemeltető a 4. § (2) bekezdésében meghatározott kockázatelemzésen alapuló üzletmenet-folytonossági tervvel és katasztrófa-helyreállítási tervvel rendelkezik, amelyek az intézkedésre jogosult, felelős személyek megjelölésével részletes akcióterveket tartalmaznak. A rendszerüzemeltető a hatályos üzletmenet-folytonossági terv és katasztrófa-helyreállítási terv érintettek számára történő elérhetőségét a teljesértékű helyszíneken folyamatosan biztosítja.

(2) Az üzletmenet-folytonossági terv és a katasztrófa-helyreállítási terv meghatározza a kockázati szintekkel arányos katasztrófaelhárítási és újraindítási eljárásokat.

(3) Az üzletmenet-folytonossági terv és a katasztrófa-helyreállítási terv és az ezekben leírt intézkedések a rendkívüli események bekövetkezése esetére oly módon biztosítják az (5) bekezdésben meghatározott katasztrófaelhárítási és újraindítási idő teljesülését, hogy a rendszerüzemeltető a részleges vagy teljes áttelepülés során a fizetési rendszer működtetésére vállalt kritikus szolgáltatását (mind a transzfer megbízás, mind az egyéb üzenetek tekintetében) megfelelő minőségben a szolgáltatáskiesés napjának végéig teljesíteni tudja akár extrém körülmények között is, kivéve a megszakítás nélkül üzemelő fizetési rendszereket.

(4) A rendszerüzemeltető a fizetési rendszer működése kapcsán elvárt katasztrófaelhárítási és újraindítási idő meghatározásakor figyelembe veszi a fizetési rendszer szabályait, így különösen a szolgáltatás jellegét.

(5) A rendszerüzemeltető a fizetési rendszer működése kapcsán elvárt katasztrófaelhárítási és újraindítási időt úgy állapítja meg, hogy az biztosítsa

a) a napi egy elszámolási és teljesítési ciklust alkalmazó fizetési rendszer esetén az adott elszámolási napra vonatkozóan érkező, minden transzfer megbízás és egyéb üzenet tekintetében a fizetési rendszerre vonatkozó szabályoknak megfelelő szolgáltatásnyújtást a következő elszámolási napnak az elszámolóház üzletszabályzatában meghatározott kezdetét megelőzően,

b) a napi több elszámolási és egy vagy több teljesítési ciklust, illetve folyamatos elszámolást és teljesítést alkalmazó fizetési rendszer esetén a rendkívüli esemény bekövetkezésétől számított két órán belüli újraindítást.

(6) A rendszerüzemeltető az üzletmenet-folytonossági tervben és a katasztrófa-helyreállítási tervben meghatározza

a) az egyes teljesértékű helyszínek működtetésbe történő bevonásának rendjét,

b) fizetési rendszer krízishelyzetben történő működtetését biztosító erőforrások - ideértve a jól képzett munkaerőt - egyes elemeit és egészét,

c) az akciótervek tesztkörnyezetét és tesztelési - de legalább évenkénti - gyakoriságát, valamint

d) azok dokumentált felülvizsgálatának gyakoriságát és eljárási rendjét.

(7) A rendszerüzemeltető ismerteti a rendszerüzemeltető irányítási jogkörrel rendelkező vezető testülete számára az üzletmenet-folytonossági és a katasztrófa-helyreállítási terv teszteredményeit.

(8) A rendszerüzemeltető biztosítja az üzletmenet-folytonossági terv és a katasztrófa-helyreállítási terv lebonyolításában érintett minden munkavállaló - a munkába lépést követően a fizetési rendszer működtetésével kapcsolatos munkavégzés megkezdése előtti, valamint a továbbiakban rendszeres - üzletmenet-folytonossági és katasztrófaelhárítási oktatását.

(9) Az üzletmenet-folytonossági tervet kiegészíti a krízishelyzetben alkalmazandó döntéshozatali és kommunikációs terv, amely a krízishelyzet hatékony kezelését biztosító módon tartalmazza

a) az egyes döntési pontokat és az azokhoz kapcsolódó döntési jogköröket,

b) a döntési jogköröket gyakorlók és helyettesük legalább két, egymástól független módon történő elérhetőségét,

c) a magasabb döntéshozatali szintre való utalás eljárását és

d) a terv tesztelésének gyakoriságát, formáját és hatókörét.

(10) A fizetési rendszer működését érintő változások során a változáskezelési eljárás tartalmazza az üzletmenet-folytonosságot és katasztrófaelhárítást befolyásoló szempontokat és terveket.

(11) A rendszerüzemeltető a rendkívüli események kapcsán trendelemzést és az alapján akciótervet készít.

27. § (1) A rendszerüzemeltető a kulcsemberkockázatot a 4. § (2) bekezdése szerint végzett kockázatelemzés során értékeli, és a 4. § (2) bekezdés *d)* pontja szerint meghatározott kockázati szinttel arányos lépéseket tesz a kockázat csökkentése érdekében.

(2) A rendszerüzemeltető olyan emberierőforrás-gazdálkodást folytat, ami alacsony szinten tartja a humán erőforrásokból fakadó kockázatokat. A rendszerüzemeltető a fizetési rendszer működtetése kapcsán biztosítja, hogy a fizetési rendszer működtetéséhez szükséges ismeret és tudás ne koncentrálódjon egyetlen személynél olyan mértékben, hogy a személy kiesése a fizetési rendszer zökkenőmentes működését veszélyeztetné.

28. § Amennyiben a rendszerüzemeltető nem azonos a teljesítő féllel, akkor mind a rendszerüzemeltető, mind a teljesítő fél úgy határozza meg üzletmenet-folytonossági és katasztrófaelhárítási eljárásait, hogy azok kölcsönösen támogassák a fizetési rendszer működtetése tevékenység jelen rendeletben meghatározott, a másik fél által végzett feladatainak végrehajthatóságát.

6. Az MNB engedélyezési eljárása

29. § Az e rendeletben foglaltaknak való megfelelést bizonyító okiratokat a rendszerüzemeltető a Hpt. szerinti engedélyezési eljáráshoz benyújtja.

7. Záró rendelkezések

30. § (1) Ez a rendelet 2022. március 1-jén lép hatályba.

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