Vezetői körlevél

az eszközalapú tokenektől és az elektronikuspénz-tokenektől eltérő kriptoeszközök ajánlattevői és az ilyen kriptoeszközök kereskedésbe történő bevezetését kérelmező személyek által fenntartandó rendszerek és biztonsági hozzáférési protokollok karbantartásáról

A Magyar Nemzeti Bank (a továbbiakban: **MNB**) a pénzügyi közvetítőrendszer stabilitása, zavartalan, átlátható, hatékony működésének biztosítása, valamint a pénzügyi közvetítőrendszer valamennyi szereplőjének védelme érdekében a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény rendelkezései alapján ellátja a pénzügyi közvetítőrendszer, ezen belül a kriptoeszközök piacáról szóló 2024. évi VII. törvény (a továbbiakban: **Kriptotv**.) hatálya alá tartozó szervezetek, személyek és tevékenységek felügyeletét, ennek körében a kriptoeszközök piacairól szóló rendelet[1] (a továbbiakban: **Rendelet**) végrehajtását.

A vezetői körlevél címzettjei a Magyarországon székhellyel, fiókteleppel rendelkező, valamint az Európai Unió más tagállamában bejegyzett vagy letelepedett, és Magyarországon létesített tartós üzleti egységük révén az ügyfelek számára állandó belföldi jelenlét formájában közvetlenül szolgáltatást kínáló, az eszközalapú tokenektől és az elektronikuspénz-tokenektől eltérő kriptoeszközök – Rendelet 3. cikk (1) bekezdés 13. pontja szerinti, valamint a Kriptotv. hatálya alá tartozó – ajánlattevői és az ilyen kriptoeszközök kereskedésbe történő bevezetését kérelmező személyek (a továbbiakban együtt: **ajánlattevő és kereskedésbe történő bevezetést kérelmező személy**).

Az Európai Értékpapír-piaci Hatóság (a továbbiakban: **ESMA**) a Rendelet 14. cikk (1) bekezdés d) pontja szerinti, az eszközalapú tokenektől és az elektronikuspénz-tokenektől eltérő kriptoeszközök ajánlattevői és az ilyen kriptoeszközök kereskedésbe történő bevezetését kérelmező személyek számára a rendszerek és a biztonsági hozzáférési protokollok karbantartására vonatkozó uniós standardok meghatározásáról iránymutatásokat (ESMA75-223375936-6132)[2] tett közzé (a továbbiakban: **ESMA Iránymutatás**).

A vezetői körlevél célja az ESMA Iránymutatásban foglaltak figyelembevételével az eszközalapú tokenektől és az elektronikuspénz-tokenektől eltérő kriptoeszközök ajánlattevői és az ilyen kriptoeszközök kereskedésbe történő bevezetését kérelmező személyek által fenntartandó rendszerek és biztonsági hozzáférési protokollok karbantartása tekintetében az MNB elvárásainak megfogalmazása, és ezzel a jogalkalmazás kiszámíthatóságának növelése, a vonatkozó jogszabályok egységes alkalmazásának elősegítése.

A jelen vezetői körlevél alkalmazásában

1.1. Hálózati és információs rendszer: a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 4. § 24. pontjában meghatározott fogalom.
1.2. Hozzáférés-ellenőrzés: annak biztosítását célzó ellenőrzések, hogy az információs és kommunikációs technológiai (a továbbiakban: **IKT**) eszközökhöz való fizikai és logikai hozzáférés engedélyezése és korlátozása üzleti és információbiztonsági követelmények alapján történjen.[3]

---

[1] a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról szóló 2023. május 31-i (EU) 2023/1114 európai parlamenti és tanácsi rendelet

[2] https://www.esma.europa.eu/sites/default/files/2025-02/ESMA75-223375936-6132_Guidelines_on_maintenance_of_systems_and_security_access_protocols_under_MiCA_HU.pdf

[3] ISO/IEC 29146:2016 Információtechnológia – Biztonsági technikák – A hozzáférés-kezelés keretrendszere. Nemzetközi Szabványügyi Szervezet, 2016.

1.3. IKT-eszköz: a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról szóló, 2022. december 14-i európai parlamenti és tanácsi (EU) 2022/2554 rendelet (a továbbiakban: **DORA-rendelet**) 3. cikk 7. pontjában meghatározott fogalom.
1.4. IKT-kockázat: a DORA-rendelet 3. cikk 5. pontjában meghatározott fogalom.

Eltérő rendelkezés hiányában a Rendeletben és a Kriptotv.-ben használt és meghatározott fogalmak a jelen vezetői körlevélben is az ott használt jelentéssel bírnak.

Az MNB elvárja, hogy az ajánlattevő és kereskedésbe történő bevezetést kérelmező személy eljárásait és szabályzatait a jelen vezetői körlevél elvárásait is figyelembevéve alakítsa ki.

A rendszerek és a biztonsági hozzáférési protokollok karbantartására vonatkozó elvárások

1. Az arányosság általános elve

Az MNB elvárása szerint az ajánlattevő és a kereskedésbe történő bevezetést kérelmező személy minden erőfeszítést megtesz annak érdekében, hogy megfeleljen a jelen vezetői körlevélben rögzített elvárásoknak oly módon, hogy az arányos legyen a szervezet méretével, átfogó kockázati profiljával, valamint tevékenységeinek vagy műveleteinek jellegével, körével és összetettségével, és figyelembe vegye azokat.

2. A rendszerekre és a biztonsági hozzáférési protokollokra vonatkozó igazgatási rendelkezések

Igazgatási rendelkezések

Elvárt, hogy az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy gondoskodjon megfelelő belső irányítási és belső ellenőrzési keretrendszer működtetéséről hálózati és információs rendszereinek karbantartásához és az IKT-kockázatok csökkentéséhez. Az ajánlattevőnek, illetve a kereskedésbe történő bevezetést kérelmező személynek továbbá egyértelmű szerep- és felelősségi köröket szükséges meghatároznia az IKT-kockázatok kezeléséért felelős feladatkörökhöz.

Az ajánlattevőnek, illetve a kereskedésbe történő bevezetést kérelmező személynek biztosítania szükséges, hogy személyzetének készségei és költségvetési forrásai megfelelőek legyenek az IKT-kockázatok kezelését célzó rendelkezések folyamatos támogatásához, különös tekintettel a hálózati és információs rendszerek karbantartásáért és a hozzáférés-ellenőrzésért felelős személyzetre. Ezen túlmenően az ajánlattevőnek, illetve a kereskedésbe történő bevezetést kérelmező személynek biztosítania szükséges, hogy az érintett személyzet tagjai – többek között a kiemelten fontos feladatkört betöltő személyek – rendszeres időközönként megfelelő képzésben részesüljenek az IKT-kockázatokról.

Az MNB elvárja, hogy az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy vezető testülete legyen számonkérhető az IKT-kockázatok kezelését célzó szervezeti rendelkezések végrehajtásának meghatározásáért, jóváhagyásáért és felügyeletéért, többek között a hálózati és információs rendszerek és a hozzáférés-ellenőrzések tekintetében.

Szerep- és felelősségi körök

Elvárt, hogy az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy a szervezeten belüli személyzetre bízza az IKT-kockázatok megfelelő azonosításának, kezelésének és felügyeletének felelősségét. Ennek biztosítania szükséges, hogy az IKT-kockázatok és a biztonsági műveletek irányításáért

felelős személyzet megfelelő eszközökkel rendelkezzen az adott IKT-kockázatok azonosításához, nyomon követéséhez, értékeléséhez és az azokról való jelentéstételhez.

Az ajánlattevőnek, illetve a kereskedésbe történő bevezetést kérelmező személynek biztosítania szükséges, hogy a hálózati és információs rendszerekhez kapcsolódó IKT-kockázatok kezeléséért és a hozzáférés-ellenőrzésekért felelős személyzet gondoskodjon az azonosított IKT-kockázatok nyomon követéséről, értékeléséről és a vezető testületnek történő jelentéséről.

Az MNB elvárja, hogy az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy meghatározza és kijelölje a kiemelten fontos hatásköröket és felelősségi köröket az alábbiakra vonatkozó rendelkezések kialakítása érdekében:

a) a szervezetet érintő IKT-kockázatok – többek között a harmadik fél szolgáltatók által nyújtott IKT-szolgáltatásokkal kapcsolatos kockázatok – azonosítása és értékelése;
b) kockázatcsökkentő intézkedések meghatározása, beleértve a harmadik féltől eredő IKT-kockázatok csökkentését célzó ellenőrzéseket;
c) a b) pontban említett intézkedések hatékonyságának nyomon követése, és szükség esetén az intézkedések javítását célzó fellépés;
d) jelentéstétel a vezető testületnek az IKT-kockázatokról és a kockázatcsökkentő intézkedésekről;
e) annak megállapítása és értékelése, hogy felmerülnek-e IKT-kockázatok a hálózati és információs rendszerek vagy az IKT-szolgáltatások bármely jelentős változása miatt (ideértve azokat az eseteket is, amikor azokat harmadik fél nyújtja) vagy bármilyen jelentős működési vagy biztonsági eseményt követően;
f) a kriptográfiai kulcsok kezelése azok teljes életciklusa során.

3. Fizikai biztonsági hozzáférési protokollok

Elvárt, hogy az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy fizikai biztonsági intézkedéseket határozzon meg, dokumentáljon és hajtson végre annak érdekében, hogy megvédje helyiségeit, adatközpontjait és érzékeny területeit a jogosulatlan hozzáféréstől és a környezeti veszélyektől. Az ajánlattevőnek, illetve a kereskedésbe történő bevezetést kérelmező személynek nyilvántartást szükséges vezetnie a hozzáférési jogosultsághoz kötött helyiségekbe való minden egyes belépésről.

A hálózati és információs rendszerekhez való fizikai hozzáférés csak az arra jogosult személyek számára engedélyezhető a szükséges ismeret és a legkevesebb jogosultság elve szerint, valamint eseti alapon. A jogosultságot a jogosult személy feladatainak és felelősségi köreinek megfelelően szükséges kiosztani, és megfelelően képzett és nyomon követett személyekre szükséges korlátozni. A fizikai hozzáférés rendszeres időközönként felülvizsgálandó és visszavonandó, ha annak fenntartása már nem indokolt.

Elvárt, hogy a környezeti veszélyekkel szembeni védelmet célzó megfelelő intézkedések arányosak legyenek az épületek jelentőségével, valamint a műveletek, illetve az épületekben lévő hálózati és információs rendszerek kritikus jellegével.

4. A hálózati és információs rendszerek biztonsági hozzáférési protokolljai

A hálózati és információs rendszerekhez való logikai hozzáférést korlátozni szükséges, az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy által kijelölt, jogosult személyek körére. A jogosultságot a személyzet feladatainak és felelősségi köreinek megfelelően szükséges kiosztani, és azon

személyekre szükséges korlátozni, akik megfelelő képzettséggel rendelkeznek, és akiknek a rendszerekhez való hozzáférését nyomon követik. Elvárt, hogy az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy olyan ellenőrzéseket vezessen be, amelyek a hálózati és információs rendszerekhez való hozzáférést megbízható módon a jogos üzleti követelményekkel rendelkező személyekre korlátozzák. Az alkalmazások adatokhoz és rendszerekhez való elektronikus hozzáférése a szükséges szolgáltatások nyújtásához szükséges minimumra korlátozandó.

Az MNB elvárja, hogy az ajánlattevő és a kereskedésbe történő bevezetést kérelmező személy a privilegizált rendszer-hozzáférésre irányuló szigorú ellenőrzéseket vezessen be, mégpedig a magas szintű rendszer-hozzáférési jogosultságokkal rendelkező személyzet szigorú korlátozásával és szoros felügyeletével. A végrehajtandó ellenőrzések például a következők: szerepalapú hozzáférés, a privilegizált felhasználók hálózati és információs rendszereken végzett tevékenységeinek naplózása és felülvizsgálata, erős hitelesítés és a rendellenességek nyomon követése. Az ajánlattevőnek, illetve a kereskedésbe történő bevezetést kérelmező személynek az információs vagyonelemekhez és az azokat támogató rendszerekhez való hozzáférési jogokat a szükséges ismeret és a legkevesebb jogosultság elve alapján szükséges kezelnie. A logikai hozzáférési jogok rendszeres időközönként felülvizsgálandók, és visszavonandók, ha azokra már nincs szükség.

A hozzáférési naplókat az azonosított üzleti funkciók, támogató folyamatok és információs vagyonelemek kritikus jellegével arányos ideig szükséges megőrizni, az uniós és a nemzeti jogban meghatározott megőrzési követelmények sérelme nélkül. Elvárt, hogy az ajánlattevő és a kereskedésbe történő bevezetést kérelmező személy ezeket az információkat felhasználja a szolgáltatásai nyújtása során észlelt rendellenes tevékenységek azonosításának és kivizsgálásának megkönnyítéséhez.

A kritikus IKT-eszközökhöz való távoli adminisztratív hozzáférés csak a szükséges ismeret és a legkevesebb jogosultság elve alapján, és kizárólag akkor biztosítható, ha rendelkezésre állnak erős hitelesítési megoldások.

A hozzáférés-ellenőrzési folyamatokhoz kapcsolódó termékek, eszközök és eljárások működésének védelmet szükséges biztosítania az adott hozzáférés-ellenőrzési folyamatok veszélyeztetésével vagy kijátszásával szemben. Ez magában foglalja a megfelelő termékek, eszközök és eljárások regisztrálását, átadását, visszahívását és visszavonását.

5. A kriptográfiai kulcsok kezelése

Az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy az IKT-kockázat tekintetében kiemelten fontos személyzethez rendelt hatáskörök és felelősségi körök részeként felel a kriptográfiai kulcsok kezeléséért. Az ajánlattevő, illetve a kereskedésbe történő bevezetést kérelmező személy IKT-kockázat tekintetében kiemelten fontos személyzete felel a kriptográfiai kulcsok kezeléséért azok teljes életciklusa során, beleértve a kulcsok generálását, megújítását, tárolását, biztonsági mentését, archiválását, visszaállítását, továbbítását, bevonását, visszavonását és megsemmisítését.

Elvárt, hogy az ajánlattevő és a kereskedésbe történő bevezetést kérelmező személy azonosítsa és végrehajtsa azokat az ellenőrzéseket, amelyek a kriptográfiai kulcsok teljes életciklusa során védelmet biztosítanak az elvesztéssel, a jogosulatlan hozzáféréssel, a nem szándékolt módon ismertté válással és módosítással szemben.

Az ajánlattevőnek és a kereskedésbe történő bevezetést kérelmező személynek az elveszett, veszélyeztetett vagy sérült kriptográfiai kulcsok helyettesítésére szolgáló módszereket szükséges kidolgoznia és végrehajtania.

Az MNB elvárja, hogy az ajánlattevő és a kereskedésbe történő bevezetést kérelmező személy legalább a kritikus IKT-eszközök összes tanúsítványa és tanúsítványtároló berendezése esetében nyilvántartást készítsen és vezessen. A nyilvántartást naprakészen szükséges tartani.

Az ajánlattevőnek és a kereskedésbe történő bevezetést kérelmező személynek a tanúsítványok lejárata előtt biztosítania szükséges azok azonnali megújítását.

***

A vezetői körlevél a felügyelt intézményekre kötelező erővel nem rendelkező felügyeleti szabályozó eszköz, azonban a vezetői körlevélben megfogalmazott elvárásoknak való megfelelést az MNB folyamatosan figyelemmel kíséri, értékeli, és a tapasztalatok alapján további szabályozói eszközök alkalmazásának szükségességét is megvizsgálja. Az MNB a jelen vezetői körlevelet a honlapján közzéteszi.

Köszönöm szíves együttműködését.

Budapest, 2026. április 22.

Dr. Sipos-Tompa Levente

a Magyar Nemzeti Bank pénzügyi szervezetek
felügyeletéért és fogyasztóvédelemért felelős alelnöke

ELEKTRONIKUSAN ALÁÍRT IRAT

Elektronikusan aláírta:
Dr. Sipos-Tompa Levente
2026.04.22. 14:50:47