PÉNZÜGYI VÁLLALKOZÁS INFORMATIKAI TÁRGYI FELTÉTELEK ENGEDÉLYEZÉSE

A működéshez szükséges tárgyi feltételek és biztonsági követelmények folyamatos biztosítása érdekében az IKT-rendszer megfelelőségét alátámasztó dokumentumok, melyekkel a pénzügyi vállalkozás igazolja, hogy olyan belső irányítási és ellenőrzési keretrendszerrel kell rendelkezniük, amely biztosítja az IKT-kockázat hatékony és prudens kezelését.

Ennek érdekében szükséges az *„Európai Parlament és a Tanács 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 2022/2554 (EU) rendelete"* **(DORA),** valamint annak 15. cikkében foglalt felhatalmazáson alapuló

„az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-kockázatkezelési eszközöket, módszereket, folyamatokat és szabályzatokat, valamint az egyszerűsített IKT-kockázatkezelési keretrendszert meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló (EU) 2024/1774 rendelet" **(RMF RTS)** alapján az IKT-rendszerek biztonságával kapcsolatos irányítási, szervezeti és szabályozási rendszer, valamint a működésbiztonság bemutatása az alábbi dokumentumokkal:

a.) az információbiztonsági célkitűzések elérésére vonatkozó stratégia és éves informatikai beruházási és költség tervek az RMF RTS 28. cikk (2) a); c) és e) pontja szerint;
b.) Szervezeti és működési szabályzat az RMF RTS 28. cikk (2) b) pontja szerint;
c.) a harmadik fél IKT-szolgáltató tevékenységét szabályozó szerződések vagy megállapodások, továbbá az ilyen szolgáltatások igénybevételét biztosító belső eljárásrendek; a kockázatok kezelését és a szolgáltatásfolytonosságot, valamint az elszámoltathatóságot biztosító technológiai és szervezési megoldások ismertetése, továbbá a harmadik fél IKT-szolgáltatók szerződései és nyilvántartása az RMF RTS 30. cikk (2) bekezdés szerint;
d.) az IKT-vonatkozású funkciók egyértelmű kijelölését biztosító dokumentumok (adatgazda és rendszergazda kijelölések az RMF RTS 28. cikk (2) b) pontja szerint;
e.) az egyszerűsített IKT-kockázatkezelési keretrendszerre vonatkozó ellenőrzési terv az RMF RTS 28. cikk (3)-(5) bekezdése alapján;
f.) Üzleti hatáselemzés (BIA) és adatvagyonleltár az RMF RTS 30. cikk (1)-(2) bekezdés és a 39. cikk 2 bekezdése szerint;
g.) Az egyszerűsített IKT-kockázatkezelési keretrendszer részeként kialakított stratégiák, szabályzatok, eljárások, IKT-protokollok RMF RTS 29. és 30-38. cikkek szerint;
h.) az egyszerűsített IKT-kockázatkezelési keretrendszer részeként az RMF RTS 29. és 30-38. cikkek szerint kialakított informatikai rendszerek ismertetése az alábbi tartalommal:
   i.) az IKT-rendszerek architektúrája és a hálózat elemei,
   ii.) a nyújtott üzleti tevékenységeket támogató üzleti informatikai rendszerek,
   iii.) a szervezetet és az ügyvitelt támogató informatikai rendszerek (például a számviteli, a törvényes beszámolási rendszerek, a munkaerő-gazdálkodás, az ügyfélkapcsolatok kezelése, az e-mail szerverek és a belső fájlszerverek),
   iv.) az engedélyezett külső kapcsolatok típusa (például kapcsolat a partnerekkel, szolgáltatókkal, a csoport más jogalanyaival és távmunkavégzésben dolgozó munkavállalóikkal, ideértve e kapcsolatok jogosságának indoklását),
   v.) az i-iv. pontokban felsorolt összes szolgáltatás esetében a bevezetett logikai biztonsági intézkedések és mechanizmusok, ideértve azt, hogy az intézmény az ilyen hozzáférés felett milyen ellenőrzéssel rendelkezik, továbbá az egyes ellenőrzések jellegét és gyakoriságát – például technikai vagy szervezeti, megelőző vagy feltáró, valós időben végzett monitoring vagy rendszeres vizsgálat, a biztonsági

berendezések konfigurálása, a kulcsok és az ügyfélazonosító igazolványok létrehozása, a rendszer monitoring, hitelesítés, a kommunikáció titkossága, a behatolások érzékelése; vírusirtó rendszerek és naplók stb. (az

vi.) az informatikai rendszerekhez való belső hozzáférést irányító logikai biztonsági intézkedések és mechanizmusok;

i.) az IKT-kockázatok részletes felmérése, amely kiterjed a harmadik fél szolgáltatókra és valamennyi, a működési környezettől való függőségből eredő kockázatra. A bevezetett vagy tervezett kockázatcsökkentő intézkedések részletes bemutatása az RMF RTS 31. cikke szerint;

j.) az IKT-rendszerek vagyonelemeinek nyilvántartási szabályai és az elemek aktuális nyilvántartásai az RMF RTS 30. cikke szerint;

k.) az IKT-rendszerek működtetése során alkalmazott megelőző védelmi és biztonsági elvek és megoldások leírása az RMF 29. cikkében foglalt elvárásnak megfelelően az alábbi tárgykörökben és részletezettséggel:

i.) az információs vagyonelemek és IKT-eszközök osztályozása (RMF RTS 30. cikk)

ii.) IKT-kockázatkezelés (RMF RTS 31. cikk)

iii.) fizikai és környezetbiztonság (RMF RTS 32. cikk)

iv.) hozzáférés-ellenőrzés (RMF RTS 33. cikk)

v.) IKT-műveletek biztonsága (RMF RTS 34. cikk), annak részeként:

a. IKT-eszközök nyilvántartása
b. beleértve a harmadik fél IKT-szolgáltatók által nyújtott szolgáltatásokat;
c. IKT-eszközök kapacitásmenedzsmentje
d. sérülékenység menedzsment;
e. patch menedzsment;
f. IKT-események naplózása;
g. IKT-műveletekkel kapcsolatos rendellenes tevékenység monitoring és kezelés;
h. kiberfenyegetések nyomon követése;
i. adatszivárgás megelőzése, vírus- és kártékonykód elleni védelem

vi.) adat-, rendszer- és hálózatbiztonság (RMF RTS 35. cikk), annak részeként:

a. adatbiztonsági intézkedések;
b. adattárolás és adatfeldolgozás biztonsága;
c. külső és belső adatkapcsolatok védelme;
d. adattovábbítás biztonsága;
e. adatok biztonságos törlése;
f. adattárolók megsemmisítése;
g. távmunka és privát eszközök használatának biztonsága

vii.) IKT-biztonsági tesztelés (RMF RTS 36. cikk);

viii.) IKT-rendszerek beszerzése, fejlesztése és karbantartása (RMF RTS 37. cikk);

ix.) IKT-projektmenedzsment és -változásmenedzsment (RMF RTS 38. cikk);

l.) a szükséges és alkalmazott szolgáltatásfolytonossági intézkedések felmérése, szabályozása, a kapcsolódó reagálási és helyreállítási tervek ismertetése, valamint szolgáltatásfolytonossági elvárásokat biztosító műszaki megoldások ismertetése az RMF RTS 39. cikke alapján (BCP, DRP tervek, kilépési stratégia);

m.) a biztonsági mentési szabályzatok és eljárások, visszaállítási és helyreállítási eljárások és módszerek, valamint az eljárások végrehajtását biztosító műszaki megoldások leírása RMF RTS 39. cikknek megfelelően;

n.) az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-vonatkozású események és kiberfenyegetések osztályozására vonatkozó kritériumokat, a lényegességi küszöbértékeket és a jelentős eseményekkel kapcsolatos bejelentések részleteit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló, a Bizottság *(EU) 2024/1772* felhatalmazáson alapuló rendelete (2024. március 13.) végrehajtását biztosító szabályozás, folyamatok és rendszereszközök dokumentumai;

o.) az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az információ-nyilvántartáshoz kapcsolódó táblák tekintetében történő alkalmazására vonatkozó végrehajtás-technikai standardok megállapításáról

szóló, a Bizottság *(EU) 2024/2956* végrehajtási rendelete (2024. november 29.) alapján létrehozott IKT-szolgáltatók nyilvántartása.

2025. január