Gyakori kérdések és válaszok informatikai szabályzatokkal kapcsolatban

1.) Mely jogszabályok és ajánlások mentén szükséges az informatikai szabályzatokat kialakítani?

- *a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (Hpt.) 67. § (1) bek. f) pontja, 67/A § / a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény (Bit.) 94. § (3)-(8) bekezdései / a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (Bszt.) 12. §, 18. § / a kollektív befektetési formákról és kezelőikről, valamint egyes pénzügyi tárgyú törvények módosításáról szóló 2014. évi XVI. törvény (Kbftv.) 18. § (3) bek., 22. §, 29-31. § /az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény (Fsztv.) 12. §, 12/A. § / az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény (Öpt.) 40/C. § /a magánnyugdíjról és a magánnyugdíjpénztárakról szóló 1997. évi LXXXII. törvény (Mpt.) 44. §, 77/A. §*
- *42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről*
- *8/2020. (VI.22.) MNB ajánlás az informatikai rendszer védelméről*
- *4/2019. (IV.1.) MNB ajánlás a közösségi és publikus felhőszolgáltatások igénybevételéről*
- *Vezetői körlevél az elektronikus úton megkötött írásbeli szerződésekről, megtett írásbeli jognyilatkozatokról*

2.) Melyek az informatikai szabályzatokkal kapcsolatban leggyakrabban felmerülő hiányosságok?

A kérelmező nem vagy nem kellő mélységben szabályozza:

- *az informatikai biztonsági kockázatelemzési és -kezelés folyamatait;*
- *a felhasználói adminisztrációs folyamatokat;*
- *a biztonsági osztályokba sorolás rendszerével kapcsolatos szabályokat és eljárásrendeket (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 szabályai, valamint azok helyreállításával és ellenőrzésével kapcsolatos szabályokat és eljárásrendeket);*
- *az információ-technológiával szemben támasztott követelményeket;*
- *a fejlesztések üzembe állítási és változtatáskezelési eljárásrendjét, a dokumentálási és jóváhagyási szabályokat, a visszaállítás eljárásait,*
- *a felhasználók tevékenységével, illetve a biztonsági eseményekkel kapcsolatos naplózás és naplókiértékelés szabályait.*

Az adminisztratív intézkedésekkel kapcsolatos hiányosságok továbbá, hogy a Kérelmező

- *nem jelöl ki adatgazdát és rendszergazdát, nem szabályozza a feladataikat és felelősségüket, illetve nem nyújtja be az erről szóló dokumentumot (amelyet az adatgazda/rendszergazda is aláírásával tudomásul vesz), az adatgazdát és a rendszergazdát nem rendeli egyértelműen össze a gondjaikra bízott vagyonelemekkel.*
- *nem nyújtja be az adatvagyon-leltárt, amelynek a Társaság által használt adatok, adatcsoportok, adatkörök besorolását kell tartalmazni a bizalmasság, sértetlenség és rendelkezésre állás alapján*
- *nem nyújt be olyan részletes helyreállítási tervet (DRP), amely katasztrófahelyzet esetén alkalmazandó, továbbá ehhez nem csatol tesztelési jegyzőkönyvet.*

*A fenti hiányosságok elkerülése érdekében kérjük figyelembe venni a Magyar Nemzeti Banknak az informatikai rendszer védelméről szóló 8/2020. (VI.22.) számú ajánlását (**Ajánlás**), különösen annak következő rendelkezéseit: 2. fejezet 3. fejezet, 9.fejezet, 1.1, 2.1, 3.1, 4.1 fejezetek és 4.4 fejezet.*

Az ajánlás teljes szövege az alábbi linken érhető el:
https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf

3.) Figyelembe kell-e venni a kérelmező működésére vonatkozó egyedi jellemzőket informatikai szabályzatainak kialakítása során?

A szabályzatokat az üzleti működést kiszolgáló informatika tényleges felépítésének, működésének figyelembevétele mellett, a napi működéssel összhangban szükséges kialakítani, így a kérelmező által elkészített szabályzatoknak illeszkednie kell a kérelmező működéséhez, az előírt gyakorlatoknak relevánsnak, életszerűnek, technikailag

kivitelezhetőnek kell lenni, illetve összhangban kell állnia a kérelmező által végezni kívánt tevékenységben rejlő kockázatokkal.

4.) Szükséges-e az egyes szabályzatok hatályát meghatározni?

Igen, az egyes szabályzatokban egyértelműen meg kell határozni azok személyi, tárgyi és területi hatályát.
A szabályozás kialakításánál kérjük figyelembe venni az Ajánlást, különösen a 2.1. fejezetet.

5.) Szükséges-e szabályzatban bemutatni az informatikai szervezetet és annak működését?

Igen, az informatikai szervezet felépítését és működését szabályzatban (pl.: a szervezeti és működési szabályzatban, IBSZ-ben) kell meghatározni.
A szabályozás kialakításánál kérjük figyelembe venni az Ajánlást, különösen az 1.2. fejezetet.

6.) Szükséges-e a szabályzatok megalkotása, az informatikai szervezet bemutatása abban az esetben, ha a teljes informatikai funkció kiszervezésre kerül?

Igen, az informatikai feltételek fennállásának bemutatására abban az esetben is szükség van, ha a kérelmező kiszervezett szolgáltatásként veszi igénybe. Ebben az esetben a fentebb hivatkozott dokumentumokon túlmenően szükséges benyújtani a kiszervezett tevékenységet végzővel kötött megbízási szerződést is, továbbá a kiszervezés tényét az üzletszabályzatban is fel kell tüntetni. A hitelintézetek és pénzügyi vállalkozások a kiszervezésre vonatkozó szerződésben foglaltaktól történő eltérő tevékenységvégzésből eredő, rendkívüli helyzetek kezelésére intézkedési tervet kell kidolgozzon. Ez az intézkedési terv nem azonos a kiszervezett tevékenységet végző saját intézkedési tervével, hanem a tervben azokat az intézkedési lépéseket kell megfogalmazni, amelyeket a hitelintézet vagy pénzügyi vállalkozás tesz meg a kiszervezett tevékenységet végző nem megfelelő munkavégzése, elérhetetlensége vagy ellehetetlenülése esetére.
Kiszervezés esetén kérjük figyelembe venni az Ajánlást, különösen a 4.5. fejezetet.

7.) Milyen rendszerben szükséges az informatikai vállalatirányítás és tervezés szabályzatait kidolgozni?

Az informatikai vállalatirányítás és tervezés szabályzatait az Ajánlás 1.1. pontjának figyelembevételével, az informatikai rendszer biztonságával kapcsolatos szabályozási rendszerben szükséges meghatározni.

8.) Hol kell a kérelmezőnek meghatároznia a kritikus védendő információk nyomon követésének (naplózás) és ellenőrzésének (kiértékelésének) szabályait?

A kérelmezőnek az informatikai biztonsági szabályzati rendjében szükséges meghatároznia a kritikus védendő információk nyomon követésének (naplózás) és ellenőrzésének (kiértékelésének) szabályait, figyelemmel az Ajánlás 14. fejezetében foglaltakra.

9.) Kell-e rendelkezni az egyes munkakörök betöltéséhez szükséges informatikai ismeretekről, és ha igen, akkor hol?

A kérelmezőnek a belső szabályzataiban kell meghatároznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet, figyelemmel az Ajánlás 2.4 fejezetére.

A kérelmező belső szabályzataiban az informatikai biztonságtudatossági oktatás szabályait is rögzíteni szükséges, tekintettel az Ajánlás 12. fejezetére.

10.) Milyen gyakran szükséges az informatikai szabályzatokat felülvizsgálni?

A szabályzatokban (vagy a szabályzatok rendszeréről szóló szabályzatban) a kérelmező rendelkezik a szabályzat felülvizsgálatának és aktualizálásának gyakoriságáról és felelőseiről, dokumentálásának eljárásrendjéről. A szabályzatokat dokumentáltan felül kell vizsgálni és aktualizálni kell minden jogszabályi, szabályozási vagy alkalmazási környezetben vagy munkafolyamatban bekövetkező lényegi változás esetén, de legkésőbb a kérelmező kockázatelemzése által előírt aktualizálásához kapcsolódóan. [Ajánlás 2.1.7.]. A szabályzatok felülvizsgálatának azonosíthatóságáról (szabályzat felülvizsgálatának vagy módosításának oka, dátuma, felelőse, változásai, jóváhagyási folyamata) és igazolhatóságáról a kérelmezőnek gondoskodnia kell.