A HITELINTÉZETEK ÉS PÉNZÜGYI VÁLLALKOZÁSOK INFORMATIKAI TÁRGYÚ SZABÁLYZATAINAK ÉS DOKUMENTUMAINAK MINIMÁLIS TARTALMI KÖVETELMÉNYEI

Dokumentum megnevezése	Tartalmi elemek	Tartalmi elemet előíró norma
IT Stratégia **Éves informatikai beruházási és költség tervek**	**Az informatikai irányítás és tervezés dokumentumai összhangban vannak az intézmény üzleti céljaival, figyelembe véve az informatikai- és adatkommunikációs technológiai irányokat. A stratégiai dokumentum az üzleti célok eléréséhez szükséges informatikai és informatikai biztonsági megoldásokat, valamint az üzleti folyamatok során alkalmazandó informatikai kontrollokat tartalmazza.** **Az IT Stratégia meghatározható hosszú (5 éven túli) és rövid (3-5 éves) távú stratégiai dokumentumokban. A stratégiában foglaltakat éves költségvetési tervekkel kell alátámasztani.**	Rendelet 2. § (1) bekezdése, 3. § (3) bekezdés a) pontja* Ajánlás 1.1 pontja**
Szervezeti és működési szabályzat	**A szervezet méretével és feladatellátásával arányos informatikai, informatikai biztonsági és informatikai ellenőrzési területek megnevezése, feladat- és hatáskörük feltüntetése**	Rendelet 2. § (3) bekezdése Ajánlás 1.2. fejezete
Kiszervezési szerződések	**A kiszervezett tevékenységet végző szervezetekkel kötött szerződések**	Hpt. 68. §, Ajánlás 4.5.
Adatgazda, rendszergazda kijelölő dokumentumok	**Az adatgazda és rendszergazda kijelölő iratokban az érintett személyeket egyértelműen össze kell rendelni a gondjaikra bízott vagyonelemekkel. A kijelölést az érintett személyek a kijelölő dokumentumban aláírásukkal tudomásul veszik. Az adatgazdák és a rendszergazdák feladatait és felelősségeit a kijelölő dokumentumban vagy szabályzatban egyértelműen meg kell határozni. Az adatgazda feladata és felelőssége nem szervezhető ki.**	Rendelet 4. § (1) bekezdés e) pontja Ajánlás 2.3. pontja
Informatikai biztonsági szabályzat	**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**	Rendelet 2. § (1), (3) bekezdése Ajánlás 2.1. pontja
	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.	Rendelet 2. § (1), (3) bekezdése Ajánlás 2.1. pontja
	A szabályzatban a kockázatokkal arányos módon ki kell térni legalább: a) az IT biztonsági kockázatelemzés és -kezelés szabályaira	Rendelet 5/B. §, Ajánlás III.-IV. fejezeteiben foglaltak

	b) az IT rendszer elemeinek egyértelmű azonosíthatóságára és dokumentáltságára; c) üzemeltetési folyamatok szabályozottságára, dokumentáltságára és ellenőrzésének eljárására; d) változáskezelésre (annak tesztelésére és dokumentálására); e) adatmentési és -visszaállítási, archiválási és tesztelési feladataira, eljárásaira f) a végfelhasználói hozzáférés szabályaira, ellenőrzésére; g) a tevékenységek naplózására a kritikus rendkívüli események riasztási módjára; h) a kiemelt jogosultságok szabályaira, dokumentáltságára, ellenőrzésére, naplózására, riasztására; i) a távoli hozzáférés szabályaira, dokumentálására, ellenőrzésére; j) a vírus és más rosszindulatú programok elleni védelemre; k) az adatkommunikációs és rendszerkapcsolatok dokumentálására, ellenőrzésére az adatkommunikáció bizalmasságára, sértetlenségére és hitelességére; l) a szolgáltatásfolytonosság és a katasztrófa-helyreállítás tervezésének szabályaira, tesztelésére; m) a rendszerek és szolgáltatások beszerzésére, azok biztonságára; n) a rendszer karbantartására; o) a rendszer adathordozóinak védelmére, ellenőrzéseire; p) a megfelelő szintű fizikai védelemről q) a biztonsági események kezeléséről; r) a rendszer üzemeltetésében és használatában részt vevő személyek rendszeres biztonságtudatossági oktatásáról, kiválasztásáról; s) az egyes -- informatikai és üzleti – munkakörök betöltéséhez szükséges konkrét informatikai és információbiztonsági ismereteket.	+ Rendelet 5. §-a
	A szabályzatban rendelkezni kell a szabályzat felülvizsgálatának és aktualizálásának gyakoriságáról és felelőseiről, dokumentálásának eljárásrendjéről. A szabályzatokat felül kell vizsgálni és aktualizálni kell minden jogszabályi, szabályozási vagy alkalmazási környezetben vagy munkafolyamatban bekövetkező lényegi változás esetén, de legkésőbb a kockázatelemzése előírt aktualizálásához kapcsolódóan.	Ajánlás 2.1.7.
Biztonsági osztályba sorolás rendszere	A kezelt adatokat, és az adatokat feldolgozó folyamatokat és rendszereket bizalmasság, sértetlenség és rendelkezésre állás alapján biztonsági osztályokba kell sorolni. A kezelt adatok vonatkozásában az egyes osztályokhoz meg kell határozni legalább a biztonsági, hozzáférési, továbbítási, tárolási, archiválási, törlési, megsemmisítési, fizikai hozzáférés-védelmi, címkézési, kódolási és szállítási feltételeket, szabályokat és eljárásokat	Rendelet 4. § (1) bekezdés c) pontja Ajánlás 2.2.

IT biztonsági kockázatelemzés és kockázatkezelés dokumentumai	Elvárható gondossággal, teljes körűen azonosítani és értékelni kell az informatikai rendszer biztonsági kockázatait az informatikai biztonsággal érintett valamennyi területen (informatikai vállalatirányítás, tervezés, fejlesztés, beszerzés, üzemeltetés, monitorozás, független ellenőrzés).	Rendelet 2. § (1), (2), (3) bekezdése Rendelet 5/A. § (3) bekezdés c) pontja Ajánlás 3. pontja
	A kockázatfelmérés során azonosított releváns kockázatokat a bekövetkezési valószínűségük és hatásuk alapján osztályozni kell, a kockázatfelmérés eredményét – beleértve az osztályozást –az informatikai biztonsági szabályozási rendszerében meghatározottak szerint kell dokumentálni és a döntéshozókkal jóvá kell hagyatni	
	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; f) elvégzésével a biztonsági hiányosságok és elégtelenségek azonosítása és a kockázatok értékelése, dokumentálása; g) 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 és bevált gyakorlatokat; h) a szabályzati előírások és a gyakorlat összhangjának a vizsgálata;	

	i) az intézmény kritikus informatikai környezetére vonatkozó informatikai biztonsági helyzetkép kialakítása, és a kockázatfelmérési jelentés dokumentum elkészítése; j) 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; k) a kockázatok feltárását követően a kockázatelemzést végző és a vizsgált terület egyeztet az esetleges téves megállapítások és az eltérő kockázati értékelések feltárása érdekében; l) k) a kockázatfelmérési jelentést – legalább vezetői összefoglaló szinten – az intézmény felső vezetése tárgyalja és hagyja jóvá.	
	A kockázatfelmérés során azonosított és osztályozott kockázatok kezelésére dokumentált és elfogadott intézkedési tervvel (felelősök, határidők megjelölésével) kell rendelkezni. A nem kezelendő kockázatokat dokumentáltan fel kell vállalni. Nem vállalhatók fel jogszabályi rendelkezések betartásával kapcsolatos kockázatok.	
	Az egyes kockázatok kezelésére előírt véghatáridők nem nyúlhatnak túl a következő kockázatelemzés előírt időpontján	
	Az üzleti folyamatokban, az informatikai rendszerben, a releváns jogszabályokban vagy szabályozási rendben bekövetkezett változás esetén az intézmény a változással érintett területen haladéktalanul, de minden terület vonatkozásában legkésőbb 2 évente felülvizsgálja és aktualizálja.	
Fejlesztési dokumentációk	Rendelkezni kell 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. 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.	Rendelet 3. § (3) bekezdés b) pontja, 4. § (1) bekezdés a) és b) pontja Ajánlás 4. pontja

Felhasználásra és üzemeltetésre vonatkozó kézikönyvek és operatív utasítások	Rendelkezni kell az informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, amelyeknek 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, illetve 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.	Rendelet 3. § (3) bekezdés a) pontja Ajánlás 5.1. pontja
IT vagyonelemek nyilvántartási dokumentumai	A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról. Biztosítani kell továbbá, hogy az élesüzemi rendszer elemei azonosíthatók és dokumentáltak legyenek.	Rendelet 3. § (2) bekezdés a) pontja Ajánlás 5. pontja
	Mindenkor rendelkezésre kell állnia az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának, valamint az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek.	Rendelet 4. § (1) bekezdés f), g) pontja Ajánlás 5. pontja
	Architektúra ábra, IT rendszer fizikai és logikai kapcsolatainak feltüntetésével, adatkapcsolatokkal, alkalmazott protokollokkal, átjárási szabályokkal. Fő- és tartalék feldolgozási és üzemeltetési helyszínek és igénybe vett külső szolgáltatók feltüntetésével.	Rendelet 5/B. § j) pontja Ajánlás 7. pontja
	Aktuális géptermi elrendezési rajzok	
Szolgáltatásfolytonossági terv (BCP), Katasztrófát követő helyreállítási terv (DRP)	Szolgáltatásfolytonosságra és katasztrófát követő helyreállításra vonatkozó teljes körű Intézkedési tervek, feladatok, felelősök, határidők, infrastruktúra megnevezéssel, elérhetőségek biztosításával	Rendelet 3. § (3) bekezdés c) f) g) pontja Ajánlás 10-11 pontjai
	Az üzleti folyamatok kritikus helyreállítási idejének (RTO) és kritikus helyreállítási pontjának (RPO) meghatározása.	
	A szolgáltatásfolytonossági intézkedési tervek és a katasztrófát követő helyreállítási tervek, valamint a mentésből történő visszaállítási tervek valós teszteléséről szóló jegyzőkönyvek, tesztelés kiértékelésével (RTO időn belül sikerült-e legalább RPO adatokkal helyreállni)	
Független ellenőrzés	Az IT szolgáltatási területek teljes körű, független, szakértői ellenőrzési tervei, határidőkkel, feladatokkal, felelősökkel.	Rendelet 2. § (3) bekezdése, 3. § (2) bekezdés b) pontja Ajánlás 13. pontja
	Az ellenőrzések során tapasztaltak kiértékelése, intézkedési terv	

	Kiszervezett tevékenységek ellenőrzése	Hpt. 68. § (6) és (10) bekezdése, Ajánlás 15. pontja
Adatszolgáltatási teszt dokumentumok, rendszerkapcsolati dokumentumok	Adatszolgáltatási teszt dokumentumok hitelintézetek közötti fizetési rendszerhez való közvetlen csatlakozásról szóló nyilatkozatot és a csatlakozást biztosító informatikai rendszer könyvvizsgálói igazolását, vagy a közvetve történő csatlakozás elfogadásáról adott nyilatkozat központi hitelinformációs rendszerről szóló törvényben meghatározott központi hitelinformációs rendszerhez történő csatlakozásról szóló nyilatkozat	Hpt. 18. § (5) bekezdés d) pontja, 20. § (2) bekezdés h), j) k) pontjai

* Rendelet címén 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. rendeletet értjük

** Ajánlás címén az informatikai rendszer védelméről szóló a Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlását értjük