Szervezet neve:	Ecsédi Polgármesteri Hivatal	Kötelező
Szervezet törzsszáma:	15378785	Kötelező
Rendszer neve:	Polgármesteri Hivatal komplex informatikai rendszere	Kötelező
Kitöltő neve:	Horkai István	Kötelező
Kitöltés dátuma:	2017.07.01.	Kötelező

Űrlap biztonsági osztályba soroláshoz és a védelmi intézkedések kiválasztásához, a 41/2015. (VII. 15.) BM rendelet alapján	A rendszer biztonsági osztálya (ezt kell elérni):			A rendszer aktuálisan megfelel:		
	3			2		
Verzió: 3.15	Bizalmasság	Sértetlenség	Rendelkezésre állás	Bizalmasság	Sértetlenség	Rendelkezésre állás
Készült: 2015.11.02	3	3	3	2	2	2
Szerzők: Szilárd Zoltán, Benyó Pál, Juhász György, Simonyi Gyula		Megfelelt/Nem felelt meg			Teljesitett osztály	
ADMINISZTRATÍV VÉDELMI NTÉZKEDÉSEK		Nem felelt meg				
3.1.1. Szervezeti szintű alapfeladatok		Megfelelt				
3.1.2. Kockázatelemzés		Megfelelt				
3.1.3. Rendszer és szolgáltatás beszerzés		Nem felelt meg				
3.1.4. Üzletmenet- (ügymenet-) folytonosság tervezése		Megfelelt			2	
3.1.5. A biztonsági események kezelése		Nem felelt meg				
3.1.6. Emberi tényezőket figyelembe vevő - személy - biztonság		Megfelelt				
3.1.7. Tudatosság és képzés		Megfelelt				
FIZIKAI VÉDELMI INTÉZKEDÉSEK		Nem felelt meg			2	
	Bizalmasság	Sértetlenség	Rendelkezésre állás	Bizalmasság	Sértetlenség	Rendelkezésre állás
LOGIKAI VÉDELMI INTÉZKEDÉSEK	Nem felelt meg	Nem felelt meg	Nem felelt meg			
3.3.1. Általános védelmi intézkedések	Megfelelt	Megfelelt	Megfelelt			
3.3.2. Tervezés	Megfelelt	Megfelelt	Megfelelt			
3.3.3. Rendszer és szolgáltatás beszerzés	Megfelelt	Megfelelt	Megfelelt			
3.3.4. Biztonsági elemzés	Megfelelt	Megfelelt	Megfelelt			
3.3.5. Tesztelés, képzés és felügyelet	Nem felelt meg	Nem felelt meg	Nem felelt meg			
3.3.6. Konfigurációkezelés	Megfelelt	Megfelelt	Megfelelt	2	2	2
3.3.7. Karbantartás	Megfelelt	Megfelelt	Megfelelt			
3.3.8. Adathordozók védelme	Megfelelt	Megfelelt	Megfelelt			
3.3.9. Azonosítás és hitelesítés	Megfelelt	Megfelelt	Megfelelt			
3.3.10. Hozzáférés ellenőrzése	Megfelelt	Megfelelt	Megfelelt			
3.3.11. Rendszer- és információsértetlenség	Megfelelt	Megfelelt	Megfelelt			
3.3.12. Naplózás és elszámoltathatóság	Megfelelt	Megfelelt	Megfelelt			
3.3.13. Rendszer- és kommunikációvédelem	Megfelelt	Megfelelt	Megfelelt			

Polgármesteri Hivatal komplex informatikai rendszere

Pont	Kérdés	Bizalmasság	Sértetlenség	Rendelkezésre állás	Osztály
2.2.1.	az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;	Igen	Igen	Igen	1
2.2.2.	nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;	Igen	Igen	Igen	
2.2.3.	a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;	Igen	Igen	Igen	
2.3.1.	személyes adat sérülhet;	Igen	Igen	Igen	2
2.3.2.	az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;	Igen	Igen	Igen	
2.3.3.	a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;	Igen	Igen	Igen	
2.3.4.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.	Igen	Igen	Igen	
2.4.1.	különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;	Igen	Igen	Igen	3
2.4.2.	az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;	Igen	Igen	Igen	
2.4.3.	a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;	Igen	Igen	Igen	
2.4.4.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.	Igen	Igen	Igen	
2.5.1.	különleges személyes adat nagy mennyiségben sérülhet;	Nem	Nem	Nem	4
2.5.2.	személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);	Nem	Nem	Nem	
2.5.3.	az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;	Nem	Nem	Nem	
2.5.4.	a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;	Nem	Nem	Nem	
2.5.5.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.	Nem	Nem	Nem	
2.6.1.	különleges személyes adat kiemelten nagy mennyiségben sérülhet;	Nem	Nem	Nem	5
2.6.2.	emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;	Nem	Nem	Nem	
2.6.3.	a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;	Nem	Nem	Nem	
2.6.4.	az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;	Nem	Nem	Nem	
2.6.5.	a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;	Nem	Nem	Nem	
2.6.6.	az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;	Nem	Nem	Nem	
2.6.7.	a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.	Nem	Nem	Nem	

A fentiektől eltérő szempont szerint történt az osztályba sorolás, éspedig:			
Szempont:	**Bizalmasság**	**Sértetlenség**	**Rendelkezésre állás**

ADMINISZTRATÍV VÉDELMI NTÉZKEDÉSEK		
Sorszám	Intézkedés típusa	Megfelelt-e
3.1.1.	Szervezeti szintű alapfeladatok	Megfelelt
3.1.1.1.	Informatikai biztonsági szabályzat	Megfelelt
3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelős személy	Megfelelt
3.1.1.3.	Az intézkedési terv és mérföldkövei	Megfelelt
3.1.1.4.	Az elektronikus információs rendszerek nyilvántartása	Megfelelt
3.1.1.5.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	Megfelelt
3.1.2.	Kockázatelemzés	Megfelelt
3.1.2.1.	Kockázatelemzési és kockázatkezelési eljárásrend	Megfelelt
3.1.2.2.	Biztonsági osztályba sorolás	Megfelelt
3.1.2.3.	Kockázatelemzés	Megfelelt
3.1.3.	Rendszer és szolgáltatás beszerzés	Nem felelt meg
3.1.3.1.	Beszerzési eljárásrend	Megfelelt
3.1.3.2.	Erőforrás igény felmérés	Nem felelt meg
3.1.3.3.	Beszerzések	Megfelelt
3.1.3.3.2.	A védelem szempontjainak érvényesítése a beszerzés során	Nem kötelező
3.1.3.3.3.	A védelmi intézkedések terv-, és megvalósítási dokumentációi	Nem kötelező
3.1.3.3.4.	Funkciók - protokollok - szolgáltatások	Nem kötelező
3.1.3.4.	Az elektronikus információs rendszerre vonatkozó dokumentáció	Megfelelt
3.1.3.5.	Biztonságtervezési elvek	Nem kötelező
3.1.3.6.	Külső elektronikus információs rendszerek szolgáltatásai	Megfelelt
3.1.3.7.	Független értékelők	Nem kötelező
3.1.3.8.	Folyamatos ellenőrzés	Nem felelt meg
3.1.3.8.2	Független értékelés	Nem kötelező
3.1.4.	Üzletmenet- (ügymenet-) folytonosság tervezése	Megfelelt
3.1.4.1.	Üzletmenet-folytonosságra vonatkozó eljárásrend	Megfelelt
3.1.4.2.	Üzletmenet-folytonossági terv informatikai erőforrás kieséseire	Megfelelt
3.1.4.2.2.	Egyeztetés	Nem kötelező
3.1.4.2.3.	Alapfunkciók újraindítása	Nem kötelező
3.1.4.2.4.	Kritikus rendszerelemek meghatározása	Nem kötelező
3.1.4.2.5.	Kapacitástervezés	Nem kötelező
3.1.4.2.6.	Összes funkció újraindítása	Nem kötelező
3.1.4.2.7.	Alapfeladatok és alapfunkciók folyamatossága	Nem kötelező
3.1.4.3.	A folyamatos működésre felkészítő képzés	Megfelelt
3.1.4.3.2.	Szimuláció	Nem kötelező
3.1.4.4.	Az üzletmenet-folytonossági terv tesztelése	Nem kötelező
3.1.4.4.2.	Koordináció	Nem kötelező
3.1.4.4.3.	Tartalék feldolgozási helyszín	Nem kötelező
3.1.4.5.	Biztonsági tárolási helyszín	Nem kötelező
3.1.4.5.2.	Elkülönítés	Nem kötelező
3.1.4.5.3.	Üzletmenet-folytonosság elérhetősége	Nem kötelező
3.1.4.5.4.	Üzletmenetfolytonosság helyreállítás	Nem kötelező
3.1.4.6.	Tartalék feldolgozási helyszín	Nem kötelező
3.1.4.6.2.	Elkülönítés	Nem kötelező
3.1.4.6.3.	Elérhetőség	Nem kötelező
3.1.4.6.4.	Szolgáltatások priorálása	Nem kötelező
3.1.4.6.5.	Előkészület a működés megindítására	Nem kötelező
3.1.4.7.	Infokommunikációs szolgáltatások	Nem kötelező
3.1.4.7.2.	Szolgáltatások prioritása	Nem kötelező

3.1.4.7.3.	Közös hibalehetőségek kizárása	Nem kötelező
3.1.4.8.	Az elektronikus információs rendszer mentései	Megfelelt
3.1.4.8.2.	Megbízhatósági és sértetlenségi teszt	Nem kötelező
3.1.4.8.3.	Helyreállítási teszt	Nem kötelező
3.1.4.8.4.	Kritikus információk elkülönítése	Nem kötelező
3.1.4.8.5.	Alternatív tárolási helyszín	Nem kötelező
3.1.4.9.	Az elektronikus információs rendszer helyreállítása és újraindítása	Megfelelt
3.1.4.9.2.	Tranzakciók helyreállítása	Nem kötelező
3.1.4.9.3.	Helyreállítási idő	Nem kötelező
3.1.5.	A biztonsági események kezelése	Nem felelt meg
3.1.5.1.	Biztonsági eseménykezelési eljárásrend	Nem felelt meg
3.1.5.2.	Automatikus eseménykezelés	Nem kötelező
3.1.5.3.	Információ korreláció	Nem kötelező
3.1.5.4.	A biztonsági események figyelése	Megfelelt
3.1.5.5.	Automatikus nyomon követés, adatgyűjtés és vizsgálat	Nem kötelező
3.1.5.6.	A biztonsági események jelentése	Megfelelt
3.1.5.6.2.	Automatizált jelentés	Nem kötelező
3.1.5.7.	Segítségnyújtás a biztonsági események kezeléséhez	Megfelelt
3.1.5.7.2.	Automatizált támogatás	Nem kötelező
3.1.5.8.	Biztonsági eseménykezelési terv	Nem felelt meg
3.1.5.9.	Képzés a biztonsági események kezelésére	Nem felelt meg
3.1.5.9.2.	Szimuláció	Nem kötelező
3.1.5.9.3.	Automatizált képzési környezet	Nem kötelező
3.1.5.9.4.	A biztonsági események kezelésének tesztelése	Nem kötelező
3.1.5.9.4.2.	Egyeztetés	Nem kötelező
3.1.6.	Emberi tényezőket figyelembe vevő - személy - biztonság	Megfelelt
3.1.6.1	Személybiztonsági eljárásrend	Megfelelt
3.1.6.2.	Munkakörök, feladatok biztonsági szempontú besorolása	Megfelelt
3.1.6.3.	A személyek ellenőrzése	Megfelelt
3.1.6.4.	Eljárás a jogviszony megszűnésekor	Megfelelt
3.1.6.5.	Az áthelyezések, átirányítások és kirendelések kezelése	Megfelelt
3.1.6.6.	Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények	Megfelelt
3.1.6.7.	Fegyelmi intézkedések	Megfelelt
3.1.6.8.	Belső egyeztetés	Megfelelt
3.1.6.9.	Viselkedési szabályok az interneten	Megfelelt
3.1.7.	Tudatosság és képzés	Megfelelt
3.1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel	Megfelelt
3.1.7.2.	Képzési eljárásrend	Megfelelt
3.1.7.3.	Biztonság tudatosság képzés	Megfelelt
3.1.7.4.	Belső fenyegetés	Nem kötelező
3.1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés	Megfelelt
3.1.7.6	A biztonsági képzésre vonatkozó dokumentációk	Megfelelt

3.2. értékelése

FIZIKAI VÉDELMI INTÉZKEDÉSEK		
Sorszám	Intézkedés típusa	Megfelelt-e
3.2.1.2.	Fizikai védelmi eljárásrend	Megfelelt
3.2.1.3.	Fizikai belépési engedélyek	Megfelelt
3.2.1.4.	A fizikai belépés ellenőrzése	Megfelelt
3.2.1.4.2.	Hozzáférés az információs rendszerhez	Nem kötelező
3.2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	Nem kötelező
3.2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése	Nem kötelező
3.2.1.7.	A fizikai hozzáférések felügyelete	Megfelelt
3.2.1.7.2.	Behatolás riasztás, felügyeleti berendezések	Nem kötelező
3.2.1.7.3.	Az elektronikus információs rendszerekhez való hozzáférés felügyelete	Nem kötelező
3.2.1.8.	A látogatók ellenőrzése	Megfelelt
3.2.1.8.2.	Automatizált látogatói információkezelés	Nem kötelező
3.2.1.9.	Áramellátó berendezések és kábelezés	Nem kötelező
3.2.1.9.1.	Tartalék áramellátás	Nem kötelező
3.2.1.9.2.	Hosszútávú tartalék áramellátás a minimálisan elvárt működési képességhez	Nem kötelező
3.2.1.10.	Vészkikapcsolás	Nem kötelező
3.2.1.11.	Vészvilágítás	Nem felelt meg
3.2.1.12.	Tűzvédelem	Nem felelt meg
3.2.1.12.2.	Automatikus tűzelfojtás	Nem kötelező
3.2.1.12.3.	Észlelő berendezések, rendszerek	Nem kötelező
3.2.1.12.4.	Tűzelfojtó berendezések, rendszerek	Nem kötelező
3.2.1.13.	Hőmérséklet és páratartalom ellenőrzés	Nem felelt meg
3.2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	Nem felelt meg
3.2.1.14.2.	Automatizált védelem	Nem kötelező
3.2.1.15.	Be- és kiszállítás	Megfelelt
3.2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése	Nem kötelező
3.2.1.17.	Ellenőrzés	Nem kötelező
3.2.1.18.	Szállítási felügyelet	Nem kötelező
3.2.1.19.	Karbantartók	Megfelelt
3.2.1.19.2.	Karbantartás fokozott biztonsági intézkedésekkel	Nem kötelező
3.2.1.19.3.	Időben történő javítás	Nem kötelező

3.3. értékelése

Sorszám	Intézkedés típusa	Bizalmasság	Sértetlenség	Rendelkezésre állás
	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Megfelelt-e		
3.3.1.	Általános védelmi intézkedések	Megfelelt	Megfelelt	Megfelelt
3.3.1.1.	Engedélyezés	Nem kötelező	Nem kötelező	Megfelelt
3.3.1.3.	Az elektronikus információs rendszer kapcsolódásai	Megfelelt	Megfelelt	Megfelelt
3.3.1.3.2.	Belső rendszerkapcsolatok	Megfelelt	Megfelelt	Megfelelt
3.3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	Megfelelt	Megfelelt	Megfelelt
3.3.1.4.	Személybiztonság	Megfelelt	Megfelelt	Megfelelt
3.3.2.	Tervezés	Megfelelt	Megfelelt	Megfelelt
3.3.2.1.	Biztonságtervezési szabályzat	Nem kötelező	Nem kötelező	Nem kötelező
3.3.2.2.	Rendszerbiztonsági terv	Megfelelt	Megfelelt	Megfelelt
3.3.2.3.	Cselekvési terv	Megfelelt	Megfelelt	Nem kötelező
3.3.2.4.	Személyi biztonság	Megfelelt	Nem kötelező	Nem kötelező
3.3.2.5.	Információbiztonsági architektúra leírás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.3.	Rendszer és szolgáltatás beszerzés	Megfelelt	Megfelelt	Megfelelt
3.3.3.2.	A rendszer fejlesztési életciklusa	Megfelelt	Nem kötelező	Nem kötelező
3.3.3.3.	Funkciók, portok, protokollok, szolgáltatások	Megfelelt	Megfelelt	Megfelelt
3.3.3.4.	Fejlesztői változáskövetés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.3.5.	Fejlesztői biztonsági tesztelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.3.6.	Fejlesztési folyamat, szabványok és eszközök	Nem kötelező	Nem kötelező	Nem kötelező
3.3.3.7.	Fejlesztői oktatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.3.8.	Fejlesztői biztonsági architektúra és tervezés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.4.	Biztonsági elemzés	Megfelelt	Megfelelt	Megfelelt
3.3.4.1.	Biztonságelemzési eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.4.2.	Biztonsági értékelések	Megfelelt	Megfelelt	Megfelelt
3.3.4.3	Speciális értékelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.4.4.	A biztonsági teljesítmény mérése	Megfelelt	Megfelelt	Megfelelt
3.3.5.	Tesztelés, képzés és felügyelet	Nem felelt meg	Nem felelt meg	Nem felelt meg
3.3.5.1.	Tesztelési, képzési és felügyeleti eljárások	Nem felelt meg	Nem felelt meg	Nem felelt meg
3.3.5.2.	A biztonsági teljesítmény mérése	Nem felelt meg	Nem felelt meg	Nem felelt meg
3.3.5.3	Sérülékenység-teszt	Nem felelt meg	Nem felelt meg	Nem felelt meg
3.3.5.3.2.	Frissítési képesség	Nem felelt meg	Nem kötelező	Nem kötelező
3.3.5.3.3.	Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően	Nem felelt meg	Nem kötelező	Nem kötelező
3.3.5.3.4.	Privilegizált hozzáférés	Nem felelt meg	Nem felelt meg	Nem felelt meg
3.3.5.3.5.	Felfedhető információk	Nem felelt meg	Nem felelt meg	Nem felelt meg
3.3.6.	Konfigurációkezelés	Megfelelt	Megfelelt	Megfelelt
3.3.6.1.	Konfigurációkezelési eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.6.2.	Alapkonfiguráció	Megfelelt	Megfelelt	Megfelelt
3.3.6.2.2.	Áttekintések és frissítések	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.2.3.	Korábbi konfigurációk megőrzése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.2.4.	Magas kockázatú területek konfigurálása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.2.5.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.3.	A konfigurációváltozások felügyelete (változáskezelés)	Megfelelt	Megfelelt	Megfelelt
3.3.6.3.2.	Előzetes tesztelés és megerősítés	Nem kötelező	Nem kötelező	Megfelelt
3.3.6.3.3.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.4.	Biztonsági hatásvizsgálat	Megfelelt	Megfelelt	Megfelelt
3.3.6.4.2.	Elkülönített tesztkörnyezet	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.5.	A változtatásokra vonatkozó hozzáférés korlátozások	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.5.2.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.5.3.	Felülvizsgálat	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.5.4.	Aláírt elemek	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.6.	Konfigurációs beállítások	Megfelelt	Megfelelt	Megfelelt
3.3.6.6.2.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.6.3.	Reagálás jogosulatlan változásokra	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.7.	Legszűkebb funkcionalitás	Megfelelt	Megfelelt	Megfelelt
3.3.6.7.2.	Rendszeres felülvizsgálat	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.7.3.	Nem futtatható szoftverek	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.7.4.	Futtatható szoftverek	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.8.	Elektronikus információs rendszerelem leltár	Megfelelt	Megfelelt	Megfelelt
3.3.6.8.2.	Frissítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.8.3.	Jogosulatlan elemek automatikus észlelése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.8.4.	Duplikálás elleni védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.8.5.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.8.6.	Naplózás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.6.9.	Konfigurációkezelési terv	Nem kötelező	Nem kötelező	Nem kötelező

3.3.6.10.	A szoftverhasználat korlátozásai	Megfelelt	Megfelelt	Megfelelt
3.3.6.11.	A felhasználó által telepített szoftverek	Megfelelt	Megfelelt	Megfelelt
3.3.7.	Karbantartás	Megfelelt	Megfelelt	Megfelelt
3.3.7.1.	Rendszer karbantartási eljárásrend	Nem kötelező	Megfelelt	Megfelelt
3.3.7.2.	Rendszeres karbantartás	Nem kötelező	Megfelelt	Megfelelt
3.3.7.2.2.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.7.3.	Karbantartási eszközök	Nem kötelező	Nem kötelező	Nem kötelező
3.3.7.3.2.	Adathordozó ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.7.4.	Távoli karbantartás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.7.4.2.	Dokumentálás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.7.4.3.	Összehasonlítható biztonság	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.	Adathordozók védelme	Megfelelt	Megfelelt	Megfelelt
3.3.8.1.	Adathordozók védelmére vonatkozó eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.8.2.	Hozzáférés az adathordozókhoz	Megfelelt	Megfelelt	Megfelelt
3.3.8.3.	Adathordozók címkézése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.4.	Adathordozók tárolása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.5.	Adathordozók szállítása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.5.2.	Kriptográfiai védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.6.	Adathordozók törlése	Megfelelt	Nem kötelező	Nem kötelező
3.3.8.6.2.	Ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.6.3.	Tesztelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.6.4.	Törlés megsemmisítés nélkül	Nem kötelező	Nem kötelező	Nem kötelező
3.3.8.7.	Adathordozók használata	Megfelelt	Megfelelt	Megfelelt
3.3.8.7.2.	Ismeretlen tulajdonos	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.	Azonosítás és hitelesítés	Megfelelt	Megfelelt	Megfelelt
3.3.9.1.	Azonosítási és hitelesítési eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.9.2.	Azonosítás és hitelesítés	Megfelelt	Megfelelt	Megfelelt
3.3.9.2.2.	Hálózati hozzáférés privilegizált fiókokhoz	Megfelelt	Nem kötelező	Nem kötelező
3.3.9.2.3.	Hálózati hozzáférés nem privilegizált fiókokhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.2.4.	Helyi hozzáférés privilegizált fiókokhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.2.5.	Visszajátszás-védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.2.6.	Távoli hozzáférés - külön eszköz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.2.7.	Helyi hozzáférés nem privilegizált fiókokhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.2.8.	Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.3.	Eszközök azonosítása és hitelesítése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.4.	Azonosító kezelés	Megfelelt	Megfelelt	Megfelelt
3.3.9.5.	A hitelesítésre szolgáló eszközök kezelése	Megfelelt	Megfelelt	Megfelelt
3.3.9.5.2.	Jelszó (tudás) alapú hitelesítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.5.3.	Birtoklás alapú hitelesítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.5.4.	Tulajdonság alapú hitelesítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció	Nem kötelező	Nem kötelező	Nem kötelező
3.3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	Megfelelt	Megfelelt	Megfelelt
3.3.9.7.	Hitelesítés kriptográfiai modul esetén	Megfelelt	Megfelelt	Megfelelt
3.3.9.8.	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	Megfelelt	Megfelelt	Megfelelt
3.3.9.8.2.	Hitelesítésszolgáltatók tanúsítványának elfogadása	Megfelelt	Megfelelt	Megfelelt
3.3.10.	Hozzáférés ellenőrzése	Megfelelt	Megfelelt	Megfelelt
3.3.10.1.	Hozzáférés ellenőrzési eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.10.2.	Felhasználói fiókok kezelése	Megfelelt	Megfelelt	Megfelelt
3.3.10.2.2.	Automatikus kezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.2.3.	Ideiglenes fiókok eltávolítása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.2.4.	Inaktív fiókok letiltása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.2.5.	Automatikus naplózás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.2.6.	Kiléptetés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.2.7.	Szokatlan használat	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.2.8.	Letiltás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.3.	Hozzáférés ellenőrzés érvényesítése	Megfelelt	Megfelelt	Megfelelt
3.3.10.4.	Információáramlás ellenőrzés érvényesítése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.5.	A felelősségek szétválasztása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.	Legkisebb jogosultság elve	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.4.	Privilegizált fiókok	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.5.	Privilegizált funkciók használatának naplózása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.6.	Privilegizált funkciók tiltása nem privilegizált felhasználóknak	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.6.7.	Hálózati hozzáférés a privilegizált parancsokhoz	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.7.	Sikertelen bejelentkezési kísérletek	Megfelelt	Megfelelt	Megfelelt

3.3.10.8.	A rendszerhasználat jelzése	Megfelelt	Megfelelt	Megfelelt
3.3.10.9.	Egyidejű munkaszakasz kezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.10.	A munkaszakasz zárolása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.10.2.	Képernyőtakarás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.11.	A munkaszakasz lezárása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	Megfelelt	Megfelelt	Megfelelt
3.3.10.13.	Távoli hozzáférés	Megfelelt	Megfelelt	Megfelelt
3.3.10.13.2.	Ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.13.3.	Titkosítás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.13.4.	Hozzáférés ellenőrzési pontok	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.13.5.	Privilegizált parancsok elérése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.14.	Vezeték nélküli hozzáférés	Megfelelt	Megfelelt	Megfelelt
3.3.10.14.2.	Hitelesítés és titkosítás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.14.3.	Felhasználó konfigurálás tiltása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.14.4.	Antennák	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.15.	Mobil eszközök hozzáférés ellenőrzése	Megfelelt	Megfelelt	Megfelelt
3.3.10.15.2.	Titkosítás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.16.	Külső elektronikus információs rendszerek használata	Megfelelt	Megfelelt	Megfelelt
3.3.10.16.2.	Korlátozott használat	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.16.3.	Hordozható adattároló eszközök	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.17.	Információmegosztás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.10.18.	Nyilvánosan elérhető tartalom	Megfelelt	Megfelelt	Megfelelt
3.3.11.	Rendszer- és információsértetlenség	Megfelelt	Megfelelt	Megfelelt
3.3.11.2.	Rendszer- és információsértetlenségre vonatkozó eljárásrend	Nem kötelező	Megfelelt	Nem kötelező
3.3.11.3.	Hibajavítás	Nem kötelező	Megfelelt	Nem kötelező
3.3.11.3.2.	Automatizált hibajavítási állapot	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.3.3.	Központi kezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.4.	Kártékony kódok elleni védelem	Megfelelt	Megfelelt	Megfelelt
3.3.11.4.2.	Központi kezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.4.3.	Automatikus frissítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.5.	Az elektronikus információs rendszer felügyelete	Megfelelt	Megfelelt	Megfelelt
3.3.11.5.2.	Automatizálás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.5.3.	Felügyelet	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.5.4.	Riasztás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.6.	Biztonsági riasztások és tájékoztatások	Megfelelt	Megfelelt	Megfelelt
3.3.11.6.2.	Automatikus riasztások	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.7.	A biztonsági funkcionalitás ellenőrzése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.8.	Szoftver- és információsértetlenség	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.8.2.	Sértetlenség ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.8.3.	Észlelés és reagálás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.8.4.	Automatikus értesítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.8.5.	Automatikus reagálás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.8.6.	Végrehajtható kód	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.9.	Kéretlen üzenetek elleni védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.9.2.	Központi kezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.9.3.	Frissítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.10.	Bemeneti információ ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.11.	Hibakezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.11.12.	A kimeneti információ kezelése és megőrzése	Megfelelt	Megfelelt	Nem kötelező
3.3.11.13.	Memóriavédelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.	Naplózás és elszámoltathatóság	Megfelelt	Megfelelt	Megfelelt
3.3.12.1.	Naplózási eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.12.2.	Naplózható események	Megfelelt	Megfelelt	Megfelelt
3.3.12.2.2.	Felülvizsgálat	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.3.	Naplóbejegyzések tartalma	Megfelelt	Megfelelt	Megfelelt
3.3.12.3.2.	Kiegészítő információk	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.3.3.	Központi kezelés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.4.	Napló tárkapacitás	Megfelelt	Megfelelt	Megfelelt
3.3.12.5.	Naplózási hiba kezelése	Megfelelt	Megfelelt	Megfelelt
3.3.12.5.2.	Naplózási tárhely ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.5.3.	Valósidejű riasztás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.6.	Naplóvizsgálat és jelentéskészítés	Megfelelt	Megfelelt	Megfelelt
3.3.12.6.2.	Folyamatba illesztés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.6.3.	Összegzés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.6.4.	Felügyeleti képességek integrálása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.6.5.	Összekapcsolás a fizikai hozzáférési információkkal	Nem kötelező	Nem kötelező	Nem kötelező

3.3.12.7.	Naplócsökkentés és jelentéskészítés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.7.2.	Automatikus feldolgozás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.8.	Időbélyegek	Megfelelt	Megfelelt	Megfelelt
3.3.12.8.2.	Szinkronizálás	Nem kötelező	Nem kötelező	Megfelelt
3.3.12.9.	A naplóinformációk védelme	Megfelelt	Megfelelt	Megfelelt
3.3.12.9.2.	Hozzáférés korlátozása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.9.3.	Fizikailag elkülönített mentés	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.9.4.	Kriptográfiai védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.10.	Letagadhatatlansága	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.11.	A naplóbejegyzések megőrzése	Megfelelt	Megfelelt	Megfelelt
3.3.12.12.	Naplógenerálás	Megfelelt	Megfelelt	Megfelelt
3.3.12.12.2.	Rendszerszintű időalapú napló	Nem kötelező	Nem kötelező	Nem kötelező
3.3.12.12.3.	Változtatások	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.	Rendszer- és kommunikációvédelem	Megfelelt	Megfelelt	Megfelelt
3.3.13.1.	Rendszer- és kommunikációvédelmi eljárásrend	Megfelelt	Megfelelt	Megfelelt
3.3.13.2.	Alkalmazás szétválasztás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.3.	Biztonsági funkciók elkülönítése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.4.	Információmaradványok	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.5.	Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem	Nem kötelező	Nem kötelező	Megfelelt
3.3.13.6.	A határok védelme	Megfelelt	Megfelelt	Megfelelt
3.3.13.6.2.	Hozzáférési pontok	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.6.3.	Külső kommunikációs szolgáltatások	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.6.4.	Alapeseti visszautasítás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.6.5.	Távoli készülékek megosztott csatornahasználatának tiltása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.6.6.	Hitelesített proxy kiszolgálók	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.6.7.	Biztonsági hibaállapot	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.6.8.	Rendszerelemek elkülönítése	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.7.	Az adatátvitel bizalmassága	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.7.2.	Kriptográfiai vagy egyéb védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.8.	Az adatátvitel sértetlensége	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.8.2.	Kriptográfiai vagy egyéb védelem	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.9.	A hálózati kapcsolat megszakítása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.10.	Kriptográfiai kulcs előállítása és kezelése	Megfelelt	Megfelelt	Megfelelt
3.3.13.10.2.	Rendelkezésre állás	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.11.	Kriptográfiai védelem	Megfelelt	Megfelelt	Nem kötelező
3.3.13.12.	Együttműködésen alapuló számítástechnikai eszközök	Megfelelt	Nem kötelező	Nem kötelező
3.3.13.13.	Nyilvános kulcsú infrastruktúra tanúsítványok	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.14.	Mobilkód korlátozása	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.15.	Elektronikus információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.16.	Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)	Nem kötelező	Megfelelt	Nem kötelező
3.3.13.17.	Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)	Nem kötelező	Megfelelt	Nem kötelező
3.3.13.18.	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	Nem kötelező	Megfelelt	Nem kötelező
3.3.13.19.	Munkaszakasz hitelessége	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.20.	Hibát követő ismert állapot	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.21.	A maradvány információ védelme	Nem kötelező	Nem kötelező	Nem kötelező
3.3.13.22.	A folyamatok elkülönítése	Megfelelt	Megfelelt	Nem kötelező

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.1.1.	SZERVEZETI SZINTŰ ALAPFELADATOK	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.1.1.	Informatikai biztonsági szabályzat	Megfelelt		X	X	X	X	X
3.1.1.1.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.1.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;	Igen		N	N	I	N	N
3.1.1.1.1.2.	más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;	Igen		N	N	I	N	N
3.1.1.1.1.3.	gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.	Igen		N	N	I	N	N
3.1.1.1.2.	*Az informatikai biztonsági szabályzatban meg kell határozni:*	-		-	-	-	-	-
3.1.1.1.2.1.	a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát;	Igen		N	N	I	N	N
3.1.1.1.2.2.	az elektronikus információbiztonsággal kapcsolatos szerepköröket;	Igen		N	N	I	N	N
3.1.1.1.2.3.	a szerepkörhöz rendelt tevékenységet;	Igen		N	N	I	N	N
3.1.1.1.2.4.	a tevékenységhez kapcsolódó felelősséget;	Igen		N	N	I	N	N
3.1.1.1.2.5.	az információbiztonság szervezetrendszerének belső együttműködését.	Igen		N	N	I	N	N
3.1.1.1.3.	*Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:*	-		-	-	-	-	-
3.1.1.1.3.1.	kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz);	Igen		N	N	I	N	N
3.1.1.1.3.2.	biztonsági helyzet-, és eseményértékelés eljárási rendje;	Igen		N	N	I	N	N
3.1.1.1.3.3.	az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (amennyiben az érintett szervezet ilyet végez, vagy végezhet);	Igen		N	N	I	N	N
3.1.1.1.3.4.	biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását);	Igen		N	N	I	N	N
3.1.1.1.3.5.	fizikai és környezeti védelem szabályai, jellemzői;	Igen		N	N	I	N	N
3.1.1.1.3.6.	az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.);	Igen	*Kötelező*	N	N	I	N	N
3.1.1.1.3.7.	az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében;	Igen		N	N	I	N	N
3.1.1.1.3.8.	az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (amennyiben az érintett szervezetnél ez értelmezhető);	Igen		N	N	I	N	N
3.1.1.1.3.9.	üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.);	Igen		N	N	I	N	N

3.1.1.1.3.10.	az elektronikus információs rendszerek karbantartásának rendje;	Igen		N	N	I	N	N
3.1.1.1.3.11.	az adathordozók fizikai és logikai védelmének szabályozása;	Igen		N	N	I	N	N
3.1.1.1.3.12.	az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése;	Igen		N	N	I	N	N
3.1.1.1.3.13.	amennyiben az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása;	Igen		N	N	I	N	N
3.1.1.1.3.14.	az adatok mentésének, archiválásának rendje,	Igen		N	N	I	N	N
3.1.1.1.3.15.	a biztonsági események - ideértve az adatok sérülését is - bekövetkeztekor követendő eljárás, ideértve a helyreállítást;	Igen		N	N	I	N	N
3.1.1.1.3.16.	az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények.	Igen		N	N	I	N	N
3.1.1.1.4.	Az informatikai biztonsági szabályzat tartalmazza az érintett szervezet elvárt biztonsági szintjét, valamint az érintett szervezet egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.	Igen		N	N	I	N	N
3.1.1.2.	**Az elektronikus információs rendszerek biztonságáért felelős személy**	Megfelelt	*Kötelező*	X	X	X	X	X
3.1.1.2.1.	Az érintett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 13. §-ában meghatározott feladatokat.	Igen		N	N	I	N	N
3.1.1.3.	**Az intézkedési terv és mérföldkövei**	Megfelelt	*Kötelező*	0	X	X	X	X
3.1.1.3.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.1.3.1.1.	intézkedési tervet készít, ebben mérföldköveket határoz meg;	Igen		N	N	I	N	N
3.1.1.3.1.2.	***meghatározott időnként felülvizsgálja és karbantartja az intézkedési tervet:***	-		-	-	-	-	-
3.1.1.3.1.2.1.	a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján;	Igen		N	N	I	N	N
3.1.1.3.1.2.2.	ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetése érdekében;	Igen		N	N	I	N	N
3.1.1.3.1.2.3.	ha a meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.	Igen		N	N	I	N	N

3.1.1.4.	**Az elektronikus információs rendszerek nyilvántartása**	Megfelelt	*Kötelező*	X	X	X	X	X
3.1.1.4.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.1.4.1.1.	elektronikus információs rendszereiről nyilvántartást vezet;	Igen		N	N	I	N	N
3.1.1.4.1.2.	folyamatosan aktualizálja a nyilvántartást.	Igen		N	N	I	N	N
3.1.1.4.2.	***A nyilvántartás minden rendszerre nézve tartalmazza:***	-		-	-	-	-	-
3.1.1.4.2.1.	annak alapfeladatait;	Igen		N	N	I	N	N
3.1.1.4.2.2.	a rendszerek által biztosítandó szolgáltatásokat;	Igen		N	N	I	N	N
3.1.1.4.2.3.	az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett szervezet kezelésében vannak);	Igen		N	N	I	N	N
3.1.1.4.2.4.	a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;	Igen		N	N	I	N	N
3.1.1.4.2.5.	a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.	Igen		N	N	I	N	N
3.1.1.5.	**Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás**	Megfelelt	*Kötelező*	X	X	X	X	X
3.1.1.5.1.	***Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:***	-		-	-	-	-	-
3.1.1.5.1.1.	emberi, fizikai és logikai erőforrásra;	Igen		N	N	I	N	N
3.1.1.5.1.2.	eljárási és védelmi követelményszintre és folyamatra.	Igen		N	N	I	N	N

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.1.2.	KOCKÁZATELEMZÉS	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.2.1.	**Kockázatelemzési és kockázatkezelési eljárásrend**	Megfelelt	*Kötelező*	X	X	X	X	X
3.1.2.1.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.2.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési és kockázatkezelési eljárásrendet, mely a kockázatelemzési és kockázatkezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen		N	N	I	N	N
3.1.2.1.1.2.	belső szabályozásában, vagy magában a kockázatelemzési és kockázatkezelési eljárásrendről szóló dokumentumban meghatározza a kockázatelemzési és kockázatkezelési eljárásrend felülvizsgálatának és frissítésének gyakoriságát.	Igen		N	N	I	N	N
3.1.2.1.2	***Az eljárásrend kiterjed:***	-		-	-	-	-	-
3.1.2.1.2.1.	a lehetséges kockázatok felmérésére;	Igen		N	N	I	N	N
3.1.2.1.2.2.	a kockázatok kezelésének felelősségére;	Igen		N	N	I	N	N
3.1.2.1.2.3.	a kockázatok kezelésének elvárt minőségére.	Igen		N	N	I	N	N
3.1.2.2.	**Biztonsági osztályba sorolás**	Megfelelt	*Kötelező*	X	X	X	X	X
3.1.2.2.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.2.2.1.1.	jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és a 3.1.1.4. pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók;	Igen		N	N	I	N	N
3.1.2.2.1.2.	vezetője jóváhagyja a biztonsági osztályba sorolást;	Igen		N	N	I	N	N
3.1.2.2.1.3.	rögzíti a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában.	Igen		N	N	I	N	N
3.1.2.2.2.	***Elvárás:***	-		-	-	-	-	-
3.1.2.2.2.1.	a biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni;	Igen		N	N	I	N	N
3.1.2.2.2.2.	kapcsolódást kell biztosítani a 3.1.1.3. pontban foglalt intézkedési tervhez és mérföldköveihez.	Igen		N	N	I	N	N
3.1.2.3.	**Kockázatelemzés**	Megfelelt	*Kötelező*	X	X	X	X	X
3.1.2.3.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.2.3.1.1.	végrehajtja a biztonsági kockázatelemzéseket;	Igen		N	N	I	N	N
3.1.2.3.1.2.	rögzíti a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy a kockázatelemzési eljárásrendben előírt dokumentumban;	Igen		N	N	I	N	N
3.1.2.3.1.3.	a kockázatelemzési eljárásrendnek megfelelően felülvizsgálja a kockázatelemzések eredményét;	Igen		N	N	I	N	N
3.1.2.3.1.4.	a kockázatelemzési eljárásrendnek megfelelően, vagy a 3.1.1.1. pont szerinti informatikai biztonsági szabályzata keretében megismerteti a kockázatelemzés eredményét az érintettekkel;	Igen		N	N	I	N	N
3.1.2.3.1.5.	amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre;	Igen		N	N	I	N	N
3.1.2.3.1.6.	gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.	Igen		N	N	I	N	N

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.1.3.	RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.3.0.	*Jelen címben meghatározott eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást, vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.*		-	-	-	-	-	-
3.1.3.1.	Beszerzési eljárásrend	Megfelelt	*Kötelező*	0	0	X	X	X
3.1.3.1.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.3.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a beszerzési eljárásrendet, mely az érintett szervezet elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen		N	N	I	N	N
3.1.3.1.1.2.	a beszerzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.	Igen		N	N	I	N	N
3.1.3.2.	Erőforrás igény felmérés	Nem felelt meg	*Kötelező*	0	0	X	X	X
3.1.3.2.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.3.2.1.1.	az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás, vagy költségvetési tervezés részeként;	Nem		N	N	I	N	N
3.1.3.2.1.2.	elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás, vagy költségvetési tervezési dokumentumaiban.	Nem		N	N	I	N	N
3.1.3.3.	Beszerzések	Megfelelt	*Kötelező*	0	0	X	X	X
3.1.3.3.1.	*Az érintett szervezet az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:*	-		-	-	-	-	-
3.1.3.3.1.1.	a funkcionális biztonsági követelményeket;	Igen		N	N	I	N	N
3.1.3.3.1.2.	a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);	Igen		N	N	I	N	N
3.1.3.3.1.3.	a biztonsággal kapcsolatos dokumentációs követelményeket;	Igen		N	N	I	N	N

3.1.3.3.1.4.	a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;	Igen		N	N	I	N	N
3.1.3.3.1.5.	az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.	Igen		N	N	I	N	N
3.1.3.3.2.	**A védelem szempontjainak érvényesítése a beszerzés során**	**Nem kötelező**		0	0	0	X	X
3.1.3.3.2.1.	Az érintett szervezet védi az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.		***Nem kötelező***	N	N	N	N	N
3.1.3.3.2.2.	Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.			N	N	N	N	N
3.1.3.3.3.	**A védelmi intézkedések terv-, és megvalósítási dokumentációi**	**Nem kötelező**		0	0	0	X	X
	Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet.		***Nem kötelező***	N	N	N	N	N
3.1.3.3.4.	**Funkciók - protokollok - szolgáltatások**	**Nem kötelező**		0	0	0	X	X
	Az érintett szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.		***Nem kötelező***	N	N	N	N	N
3.1.3.4.	**Az elektronikus információs rendszerre vonatkozó dokumentáció**	**Megfelelt**		0	0	X	X	X
3.1.3.4.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.3.4.1.1.	***ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:***	-		-	-	-	-	-
3.1.3.4.1.1.1.	a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,	Igen		N	N	I	N	N
3.1.3.4.1.1.2.	a biztonsági funkciók hatékony alkalmazását és fenntartását,	Igen		N	N	I	N	N
3.1.3.4.1.1.3.	a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;	Igen		N	N	I	N	N
3.1.3.4.1.2.	***megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:***	-	***Kötelező***	-	-	-	-	-
3.1.3.4.1.2.1.	a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,	Igen		N	N	I	N	N
3.1.3.4.1.2.2.	a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,	Igen		N	N	I	N	N

3.1.3.4.1.2.3.	a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;	Igen		N	N	I	N	N
3.1.3.4.1.3.	gondoskodik arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;	Igen		N	N	I	N	N
3.1.3.4.1.4.	gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.	Igen		N	N	I	N	N
3.1.3.5.	**Biztonságtervezési elvek**	**Nem kötelező**	***Nem kötelező***	0	0	0	X	X
	Az érintett szervezet biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.			N	N	N	N	N
3.1.3.6.	**Külső elektronikus információs rendszerek szolgáltatásai**	**Megfelelt**	***Kötelező***	0	X	X	X	X
3.1.3.6.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.3.6.1.1.	szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek;	Igen		N	N	I	N	N
3.1.3.6.1.2.	meghatározza és dokumentálja az érintett szervezet felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;	Igen		N	N	I	N	N
3.1.3.6.1.3.	külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.	Igen		N	N	I	N	N
3.1.3.7.	**Független értékelők**	**Nem kötelező**	***Nem kötelező***	0	0	0	X	X
	Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére.			N	N	N	N	N
3.1.3.8.	**Folyamatos ellenőrzés**	**Nem felelt meg**	***Kötelező***	0	0	X	X	X
3.1.3.8.1.	***Az érintett szervezet folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:***	-		-	-	-	-	-
3.1.3.8.1.1.	az ellenőrizendő területeket;	Nem		N	N	I	N	N
3.1.3.8.1.2.	az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;	Nem		N	N	I	N	N
3.1.3.8.1.3.	az érintett szervezet ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;	Nem		N	N	I	N	N
3.1.3.8.1.4.	a mérőszámok megfelelőségét;	Nem		N	N	I	N	N
3.1.3.8.1.5.	az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;	Nem		N	N	I	N	N
3.1.3.8.1.6.	az érintett szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;	Nem		N	N	I	N	N
3.1.3.8.1.7.	az érintett szervezet döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).	Nem		N	N	I	N	N
3.1.3.8.2	**Független értékelés**	**Nem kötelező**	***Nem kötelező***	0	0	0	X	X
	Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmazhat az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére.			N	N	N	N	N

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály	3	Követelmény				
3.1.4.	ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.4.1.	Üzletmenet-folytonosságra vonatkozó eljárásrend	Megfelelt		0	X	X	X	X
3.1.4.1.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.4.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	*Kötelező*	N	N	I	N	N
3.1.4.1.1.2.	az üzletmenet-folytonossági tervben, vagy más szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az üzletmenet-folytonosságra vonatkozó eljárásrendet.	Igen		N	N	I	N	N
3.1.4.2.	Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre	Megfelelt		0	X	X	X	X
3.1.4.2.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.4.2.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet;	Igen	*Kötelező*	N	N	I	N	N
3.1.4.2.1.2.	összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;	Igen		N	N	I	N	N
3.1.4.2.1.3.	meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;	Igen		N	N	I	N	N
3.1.4.2.1.4.	az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;	Igen		N	N	I	N	N
3.1.4.2.1.5.	tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;	Igen		N	N	I	N	N
3.1.4.2.1.6.	gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;	Igen		N	N	I	N	N
3.1.4.2.1.7.	meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;	Igen		N	N	I	N	N
3.1.4.2.1.8.	rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;	Igen		N	N	I	N	N
3.1.4.2.1.9.	jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;	Igen		N	N	I	N	N
3.1.4.2.1.10.	fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;	Igen		N	N	I	N	N
3.1.4.2.1.11.	kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.	Igen		N	N	I	N	N

3.1.4.2.2.	Egyeztetés	Nem kötelező	*Nem kötelező*	0	0	0	X	X		
	Az üzletmenet-folytonossági tervet egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel.			N	N	N	N	N		
3.1.4.2.3.	Alapfunkciók újraindítása	Nem kötelező	*Nem kötelező*	0	0	0	X	X		
	Meg kell határozni az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően.			N	N	N	N	N		
3.1.4.2.4.	Kritikus rendszerelemek meghatározása	Nem kötelező	*Nem kötelező*	0	0	0	X	X		
	Meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket.			N	N	N	N	N		
3.1.4.2.5.	Kapacitástervezés	Nem kötelező	*Nem kötelező*	0	0	0	0	X		
	Meg kell tervezni a folyamatos működéshez szükséges információ-feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.			N	N	N	N	N		
3.1.4.2.6.	Összes funkció újraindítása	Nem kötelező	*Nem kötelező*	0	0	0	0	X		
	Meg kell határozni az összes funkció újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően.			N	N	N	N	N		
3.1.4.2.7.	Alapfeladatok és alapfunkciók folyamatossága	Nem kötelező	*Nem kötelező*	0	0	0	0	X		
	Az alapfeladatok és alapfunkciók folyamatosságát úgy kell megtervezni, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő, fenntartható legyen a folyamatosság az elektronikus információs rendszer elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.			N	N	N	N	N		
3.1.4.3.	A folyamatos működésre felkészítő képzés	Megfelelt	*Kötelező*	0	0	X	X	X		
3.1.4.3.1.	*Az érintett szervezet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:*	-		-	-	-	-	-		
3.1.4.3.1.1.	szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;	Igen		N	N	I	N	N		
3.1.4.3.1.2.	meghatározott gyakorisággal, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.	Igen		N	N	I	N	N		
3.1.4.3.2.	Szimuláció	Nem kötelező	*Nem kötelező*	0	0	0	0	X		
	A folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.			N	N	N	N	N		
3.1.4.4.	Az üzletmenet-folytonossági terv tesztelése	Nem kötelező	*Nem kötelező*	0	0	0	X	X		
3.1.4.4.1.	*Az érintett szervezet:*	-		-	-	-	-	-		
3.1.4.4.1.1.	meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az elektronikus információs rendszerre vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és az érintett szervezet felkészültségének a felmérése céljából;			N	N	N	N	N		
3.1.4.4.1.2.	értékeli az üzletmenet-folytonossági terv tesztelési eredményeit;			N	N	N	N	N		

3.1.4.4.1.3.	az értékelés alapján szükség esetén javítja a tervet, a javításokkal kapcsolatban az üzletmenet-folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el.			N	N	N	N	N
3.1.4.4.2.	Koordináció	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	Az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell.			N	N	N	N	N
3.1.4.4.3.	Tartalék feldolgozási helyszín	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	Az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy az érintett szervezet megismerje az adottságokat, és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.			N	N	N	N	N
3.1.4.5.	Biztonsági tárolási helyszín	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	Az érintett szervezet kijelöl egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja.			N	N	N	N	N
3.1.4.5.2.	Elkülönítés	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	A biztonsági tárolási helyszínnek el kell különülni az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.			N	N	N	N	N
3.1.4.5.3.	Üzletmenet-folytonosság elérhetőség	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	A biztonsági tárolási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.			N	N	N	N	N
3.1.4.5.4.	Üzletmenetfolytonosság helyreállítás	Nem kötelező	*Nem kötelező*	0	0	0	0	X
	A biztonsági tárolási helyszínt úgy kell kialakítani, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.			N	N	N	N	N
3.1.4.6.	Tartalék feldolgozási helyszín	Nem kötelező		0	0	0	X	X
3.1.4.6.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.4.6.1.1.	kijelöl egy tartalék feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésére, elektronikus információs rendszere előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - a tartalék helyszínen újra kezdhesse, vagy folytathassa;		*Nem kötelező*	N	N	N	N	N
3.1.4.6.1.2.	biztosítja, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek a tartalék feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak;			N	N	N	N	N
3.1.4.6.1.3.	biztosítja, hogy a tartalék feldolgozási helyszín informatikai biztonsági intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.			N	N	N	N	N

3.1.4.6.2.	**Elkülönítés**	Nem kötelező	*Nem kötelező*	0	0	0	0	X	
	Olyan tartalék feldolgozási helyszínt kell kijelölni, amely elkülönül az elsődleges feldolgozás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.			N	N	N	N	N	
3.1.4.6.3.	**Elérhetőség**	Nem kötelező	*Nem kötelező*	0	0	0	0	X	
	Az alternatív feldolgozási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.			N	N	N	N	N	
3.1.4.6.4.	**Szolgáltatások priorálása**	Nem kötelező	*Nem kötelező*	0	0	0	0	X	
	A tartalék feldolgozási helyszínre vonatkozóan olyan megállapodásokat kell kötni, intézkedéseket kell bevezetni, amelyek a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban álló szolgáltatás-prioritási rendelkezéseket tartalmaznak.			N	N	N	N	N	
3.1.4.6.5.	**Előkészület a működés megindítására**	Nem kötelező	*Nem kötelező*	0	0	0	0	X	
	Az érintett szervezet úgy készíti fel a tartalék feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.			N	N	N	N	N	
3.1.4.7.	**Infokommunikációs szolgáltatások**	Nem kötelező	*Nem kötelező*	0	0	0	X	X	
	Az érintett szervezet - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, amennyiben az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.			N	N	N	N	N	
3.1.4.7.2.	**Szolgáltatások prioritása**	Nem kötelező	*Nem kötelező*	0	0	0	X	X	
	Amennyiben az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.			N	N	N	N	N	
3.1.4.7.3.	**Közös hibalehetőségek kizárása**	Nem kötelező	*Nem kötelező*	0	0	0	X	X	
	Olyan tartalék infokommunikációs szolgáltatásokat kell igénybe venni, melyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).			N	N	N	N	N	
3.1.4.8.	**Az elektronikus információs rendszer mentései**	Megfelelt	*Kötelező*	0	X	X	X	X	
3.1.4.8.1.	***Az érintett szervezet:***	-		-	-	-	-	-	
3.1.4.8.1.1.	meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;	Igen		N	N	I	N	N	
3.1.4.8.1.2.	meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;	Igen		N	N	I	N	N	

3.1.4.8.1.3.	meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;	Igen		N	N	I	N	N
3.1.4.8.1.4.	megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.	Igen		N	N	I	N	N
3.1.4.8.2.	**Megbízhatósági és sértetlenségi teszt**	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	Meghatározott gyakorisággal tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.			N	N	N	N	N
3.1.4.8.3.	**Helyreállítási teszt**	Nem kötelező	*Nem kötelező*	0	0	0	0	X
	Az üzletmenet-folytonossági terv tesztelésének részeként egy kiválasztott mintát kell használni a biztonsági másolat információkból az elektronikus információs rendszer kiválasztott funkcióinak helyreállításánál.			N	N	N	N	N
3.1.4.8.4.	**Kritikus információk elkülönítése**	Nem kötelező	*Nem kötelező*	0	0	0	0	X
	Az érintett szervezet által meghatározott, az elektronikus információs rendszer kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak biztonsági másolatait egy elkülönített berendezésen vagy egy minősítéssel rendelkező tűzbiztos tárolóban kell tárolni.			N	N	N	N	N
3.1.4.8.5.	**Alternatív tárolási helyszín**	Nem kötelező	*Nem kötelező*	0	0	0	0	X
	Az elektronikus információs rendszer biztonsági másolat információit a 3.1.4.5. pontban meghatározottak szerinti biztonsági tárolási helyszínen kell tárolni.			N	N	N	N	N
3.1.4.9.	**Az elektronikus információs rendszer helyreállítása és újraindítása**	Megfelelt	*Kötelező*	0	X	X	X	X
	Az érintett szervezet gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.	Igen		N	N	I	N	N
3.1.4.9.2.	**Tranzakciók helyreállítása**	Nem kötelező	*Nem kötelező*	0	0	0	X	X
	Az érintett szervezet tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítást hajt végre.			N	N	N	N	N
3.1.4.9.3.	**Helyreállítási idő**	Nem kötelező	*Nem kötelező*	0	0	0	0	X
	Az érintett szervezet biztosítja azt a lehetőséget, hogy az elektronikus információs rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani egy olyan konfigurációellenőrzött és sértetlenség védett információból, ami az elem ismert működési állapotát reprezentálja.			N	N	N	N	N

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.1.5	A BIZTONSÁGI ESEMÉNYEK KEZELÉSE	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.5.1.	Biztonsági eseménykezelési eljárásrend	Nem felelt meg	Kötelező	0	0	X	X	X
3.1.5.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.5.1.1.	eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást;	Nem		N	N	I	N	N
3.1.5.1.2.	egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel;	Nem		N	N	I	N	N
3.1.5.1.3.	az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.	Nem		N	N	I	N	N
3.1.5.2.	Automatikus eseménykezelés	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet automatizált mechanizmusokat alkalmaz az eseménykezelési eljárások támogatására.			N	N	N	N	N
3.1.5.3.	Információ korreláció	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet összekapcsolja a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és reagálásokra.			N	N	N	N	N
3.1.5.4.	A biztonsági események figyelése	Megfelelt	Kötelező	0	0	X	X	X
	Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.	Igen		N	N	I	N	N
3.1.5.5.	Automatikus nyomon követés, adatgyűjtés és vizsgálat	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.			N	N	N	N	N
3.1.5.6.	A biztonsági események jelentése	Megfelelt	Kötelező	0	0	X	X	X
3.1.5.6.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.5.6.1.1.	mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek;	Igen		N	N	I	N	N
3.1.5.6.1.2.	jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek.	Igen		N	N	I	N	N
3.1.5.6.2.	Automatizált jelentés	Nem kötelező	Nem kötelező	0	0	0	X	X
	Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események jelentését.			N	N	N	N	N

3.1.5.7.	**Segítségnyújtás a biztonsági események kezeléséhez**	**Megfelelt**	***Kötelező***	0	0	X	X	X	
3.1.5.7.1.	Az érintett szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.	Igen		N	N	I	N	N	
3.1.5.7.2.	**Automatizált támogatás**	**Nem kötelező**	***Nem kötelező***	0	0	0	X	X	
	Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.			N	N	N	N	N	
3.1.5.8.	**Biztonsági eseménykezelési terv**	**Nem felelt meg**	***Kötelező***	0	0	X	X	X	
3.1.5.8.1.	***Az érintett szervezet:***	-		-	-	-	-	-	
3.1.5.8.1.1.	***kidolgozza a biztonsági eseménykezelési tervet, amely:***	-		-	-	-	-	-	
3.1.5.8.1.1.1.	az érintett szervezet számára iránymutatást ad a biztonsági esemény kezelési módjaira,	Nem		N	N	I	N	N	
3.1.5.8.1.1.2.	ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,	Nem		N	N	I	N	N	
3.1.5.8.1.1.3.	átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,	Nem		N	N	I	N	N	
3.1.5.8.1.1.4.	kielégíti az érintett szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit,	Nem		N	N	I	N	N	
3.1.5.8.1.1.5.	meghatározza a bejelentésköteles biztonsági eseményeket,	Nem		N	N	I	N	N	
3.1.5.8.1.1.6.	meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét,	Nem		N	N	I	N	N	
3.1.5.8.1.1.7.	támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,	Nem		N	N	I	N	N	
3.1.5.8.1.1.8.	meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására;	Nem		N	N	I	N	N	
3.1.5.8.1.2.	kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek;	Nem		N	N	I	N	N	
3.1.5.8.1.3.	meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet;	Nem		N	N	I	N	N	
3.1.5.8.1.4.	frissíti a biztonsági eseménykezelési tervet, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;	Nem		N	N	I	N	N	
3.1.5.8.1.5.	a biztonsági eseménykezelési terv változásait a 3.1.5.8.1.2. pont szerint ismerteti;	Nem		N	N	I	N	N	
3.1.5.8.1.6.	gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.	Nem		N	N	I	N	N	

3.1.5.9.	**Képzés a biztonsági események kezelésére**	Nem felelt meg		0	0	X	X	X
3.1.5.9.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.5.9.1.1.	biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;	Nem	*Kötelező*	N	N	I	N	N
3.1.5.9.1.2.	a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal tartja.	Nem		N	N	I	N	N
3.1.5.9.2.	**Szimuláció**	Nem kötelező		0	0	0	0	X
	Az érintett szervezet a biztonsági esemény kezelési képzésébe szimulált eseményeket foglal, hogy elősegítse a személyzet hatékony reagálását kritikus helyzetekben.		***Nem kötelező***	N	N	N	N	N
3.1.5.9.3.	**Automatizált képzési környezet**	Nem kötelező		0	0	0	0	X
	Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy biztonsági esemény kezelési képzéséhez mélyrehatóbb és valószerűbb környezetet biztosítson.		***Nem kötelező***	N	N	N	N	N
3.1.5.9.4.	**A biztonsági események kezelésének tesztelése**	Nem kötelező		0	0	0	X	X
3.1.5.9.4.1.	Az érintett szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket.		***Nem kötelező***	N	N	N	N	N
3.1.5.9.4.2.	**Egyeztetés**	Nem kötelező		0	0	0	X	X
	Az érintett szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (pl. üzletmenet-folytonossági terv és katasztrófaelhárítási terv) felelős szervezeti egységekkel.		***Nem kötelező***	N	N	N	N	N

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.1.6.	EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.6.1	**Személybiztonsági eljárásrend**	Megfelelt		0	0	X	X	X
	Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).	Igen	*Kötelező*	N	N	I	N	N
3.1.6.2.	**Munkakörök, feladatok biztonsági szempontú besorolása**	Megfelelt		0	0	X	X	X
3.1.6.2.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.6.2.1.1.	minden érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot biztonsági szempontból besorol;	Igen	*Kötelező*	N	N	I	N	N
3.1.6.2.1.2.	felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat;	Igen		N	N	I	N	N
3.1.6.2.1.3.	rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.	Igen		N	N	I	N	N
3.1.6.3.	**A személyek ellenőrzése**	Megfelelt		0	0	X	X	X
3.1.6.3.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.6.3.1.1.	az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a 3.1.6.2.1.1. és 3.1.6.2.1.2. pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e;	Igen	*Kötelező*	N	N	I	N	N
3.1.6.3.1.2.	a 3.1.6.2.1.2. szerinti munkaköröket betöltő, vagy feladatokat ellátó személyek tekintetében kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést;	Igen		N	N	I	N	N
3.1.6.3.1.3.	folyamatosan ellenőrzi a 3.1.6.3.1. pont szerinti feltételek fennállását.	Igen		N	N	I	N	N
3.1.6.4.	**Eljárás a jogviszony megszűnésekor**	Megfelelt		X	X	X	X	X
3.1.6.4.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.6.4.1.1.	belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez;	Igen		N	N	I	N	N
3.1.6.4.1.2.	megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;	Igen		N	N	I	N	N
3.1.6.4.1.3.	tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;	Igen		N	N	I	N	N
3.1.6.4.1.4.	visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;	Igen	*Kötelező*	N	N	I	N	N

3.1.6.4.1.5.	megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;	Igen		N	N	I	N	N
3.1.6.4.1.6.	az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;	Igen		N	N	I	N	N
3.1.6.4.1.7.	a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;	Igen		N	N	I	N	N
3.1.6.4.1.8.	a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.	Igen		N	N	I	N	N
3.1.6.5.	**Az áthelyezések, átirányítások és kirendelések kezelése**	**Megfelelt**		0	0	X	X	X
3.1.6.5.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.6.5.1.1.	szükség esetén elvégzi a 3.1.6.3. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást;	Igen		N	N	I	N	N
3.1.6.5.1.2.	logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt elektronikus információs rendszerhez;	Igen	*Kötelező*	N	N	I	N	N
3.1.6.5.1.3.	szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását, vagy megszüntetését;	Igen		N	N	I	N	N
3.1.6.5.1.4.	az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.	Igen		N	N	I	N	N
3.1.6.6.	**Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények**	**Megfelelt**		0	0	X	X	X
3.1.6.6.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.6.6.1.1.	a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;	Igen		N	N	I	N	N
3.1.6.6.1.2.	szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek;	Igen	*Kötelező*	N	N	I	N	N
3.1.6.6.1.3.	a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;	Igen		N	N	I	N	N
3.1.6.6.1.4.	előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek;	Igen		N	N	I	N	N
3.1.6.6.1.5.	folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.	Igen		N	N	I	N	N

3.1.6.7.	**Fegyelmi intézkedések**	Megfelelt	Kötelező	X	X	X	X	X
3.1.6.7.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.6.7.1.1.	belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;	Igen		N	N	I	N	N
3.1.6.7.1.2.	amennyiben az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.	Igen		N	N	I	N	N
3.1.6.8.	**Belső egyeztetés**	Megfelelt	Kötelező	0	0	X	X	X
	Az érintett szervezet tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.	Igen		N	N	I	N	N
3.1.6.9.	**Viselkedési szabályok az interneten**	Megfelelt	Kötelező	X	X	X	X	X
3.1.6.9.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.1.6.9.1.1.	tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;	Igen		N	N	I	N	N
3.1.6.9.1.2.	tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);	Igen		N	N	I	N	N
3.1.6.9.1.3.	tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.	Igen		N	N	I	N	N

3.1.	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.1.7.	TUDATOSSÁG ÉS KÉPZÉS	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel	Megfelelt		0	0	X	X	X
3.1.7.1.1.	*Az érintett szervezet kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével:*	-		-	-	-	-	-
3.1.7.1.1.1.	az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítése érdekében;	Igen	*Kötelező*	N	N	I	N	N
3.1.7.1.1.2.	az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása érdekében;	Igen		N	N	I	N	N
3.1.7.1.1.3.	a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében.	Igen		N	N	I	N	N
3.1.7.2.	Képzési eljárásrend	Megfelelt		X	X	X	X	X
3.1.7.2.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.1.7.2.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a képzési eljárásrendet, mely a képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	*Kötelező*	N	N	I	N	N
3.1.7.2.1.2.	a képzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.	Igen		N	N	I	N	N
3.1.7.3.	Biztonság tudatosság képzés	Megfelelt		X	X	X	X	X
3.1.7.3.1.	*Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:*	-	*Kötelező*	-	-	-	-	-
3.1.7.3.1.1.	az új felhasználók kezdeti képzésének részeként;	Igen		N	N	I	N	N
3.1.7.3.1.2.	amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;	Igen		N	N	I	N	N
3.1.7.3.1.3.	az érintett szervezet által meghatározott gyakorisággal.	Igen		N	N	I	N	N
3.1.7.4.	Belső fenyegetés	Nem kötelező		0	0	0	X	X
	A biztonságtudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.		*Nem kötelező*	N	N	N	N	N
3.1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés	Megfelelt		0	0	X	X	X
3.1.7.5.1.	*Az érintett szervezet szerepkör, vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek:*	-	*Kötelező*	-	-	-	-	-
3.1.7.5.1.1.	az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;	Igen		N	N	I	N	N
3.1.7.5.1.2.	amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;	Igen		N	N	I	N	N
3.1.7.5.1.3.	az érintett szervezet által meghatározott rendszerességgel.	Igen		N	N	I	N	N
3.1.7.6	A biztonsági képzésre vonatkozó dokumentációk	Megfelelt		0	0	X	X	X
3.1.7.6.1.	*Az érintett szervezet:*	-	*Kötelező*	-	-	-	-	-
3.1.7.6.1.1.	dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;	Igen		N	N	I	N	N
3.1.7.6.1.2.	a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi.	Igen		N	N	I	N	N

3.2.	FIZIKAI VÉDELMI INTÉZKEDÉSEK	Elvárt osztály:	3	Követelmény				
3.2.1.	FIZIKAI ÉS KÖRNYEZETI VÉDELEM	Megfelelt? (I/N)	Ki kell tölteni?	1	2	3	4	5
3.2.1.1.	***Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.***	-	-	-	-	-	-	-
3.2.1.2.	Fizikai védelmi eljárásrend	Megfelelt		0	X	X	X	X
3.2.1.2.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.2.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely az érintett szervezet elektronikus információbiztonsági, vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	*Kötelező*	N	N	I	N	N
3.2.1.2.1.2.	a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.	Igen		N	N	I	N	N
3.2.1.3.	Fizikai belépési engedélyek	Megfelelt		0	X	X	X	X
3.2.1.3.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.3.1.1.	összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;	Igen		N	N	I	N	N
3.2.1.3.1.2.	belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;	Igen	*Kötelező*	N	N	I	N	N
3.2.1.3.1.3.	rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;	Igen		N	N	I	N	N
3.2.1.3.1.4.	eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;	Igen		N	N	I	N	N
3.2.1.3.1.5.	intézkedik a 3.2.1.3.1.2. szerinti dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.	Igen		N	N	I	N	N
3.2.1.4.	A fizikai belépés ellenőrzése	Megfelelt		0	X	X	X	X
3.2.1.4.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.4.1.1.	kizárólag az érintett szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;	Igen		N	N	I	N	N
3.2.1.4.1.2.	naplózza a fizikai belépéseket;	Igen		N	N	I	N	N
3.2.1.4.1.3.	ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;	Igen		N	N	I	N	N
3.2.1.4.1.4.	kíséri a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;	Igen		N	N	I	N	N
3.2.1.4.1.5.	megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;	Igen	*Kötelező*	N	N	I	N	N
3.2.1.4.1.6.	nyilvántartást vezet a fizikai belépést ellenőrző eszközről;	Igen		N	N	I	N	N

3.2.1.4.1.7.	meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;	Igen		N	N	I	N	N
3.2.1.4.1.8.	az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;	Igen		N	N	I	N	N
3.2.1.4.1.9.	a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel;	Igen		N	N	I	N	N
3.2.1.4.1.10.	felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.	Igen		N	N	I	N	N
3.2.1.4.2.	**Hozzáférés az információs rendszerhez**	Nem kötelező		0	0	0	0	X
	Az érintett szervezet a létesítménybe történő fizikai belépés ellenőrzésén túl külön engedélyhez köti a fizikai belépést az elektronikus információs rendszereknek helyt adó helyiségekbe is.		*Nem kötelező*	N	N	N	N	N
3.2.1.5.	**Hozzáférés az adatátviteli eszközökhöz és csatornákhoz**	Nem kötelező		0	0	0	X	X
	Az érintett szervezet az általa meghatározott biztonsági védelemmel ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.		*Nem kötelező*	N	N	N	N	N
3.2.1.6.	**A kimeneti eszközök hozzáférés ellenőrzése**	Nem kötelező		0	0	0	X	X
	Az érintett szervezet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.		*Nem kötelező*	N	N	N	N	N
3.2.1.7.	**A fizikai hozzáférések felügyelete**	Megfelelt		0	0	X	X	X
3.2.1.7.1.	***Az érintett szervezet:***	-		-	-	-	-	-
3.2.1.7.1.1.	ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra;	Igen		N	N	I	N	N
3.2.1.7.1.2.	rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat;	Igen	*Kötelező*	N	N	I	N	N
3.2.1.7.1.3.	azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak;	Igen		N	N	I	N	N
3.2.1.7.1.4.	összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.	Igen		N	N	I	N	N
3.2.1.7.2.	**Behatolás riasztás, felügyeleti berendezések**	Nem kötelező		0	0	0	X	X
	Az érintett szervezet felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.		*Nem kötelező*	N	N	N	N	N
3.2.1.7.3.	**Az elektronikus információs rendszerekhez való hozzáférés felügyelete**	Nem kötelező		0	0	0	0	X
	Az érintett szervezet a létesítménybe való fizikai belépések ellenőrzésén felül külön felügyeli az elektronikus információs rendszer egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépéseket.		*Nem kötelező*	N	N	N	N	N

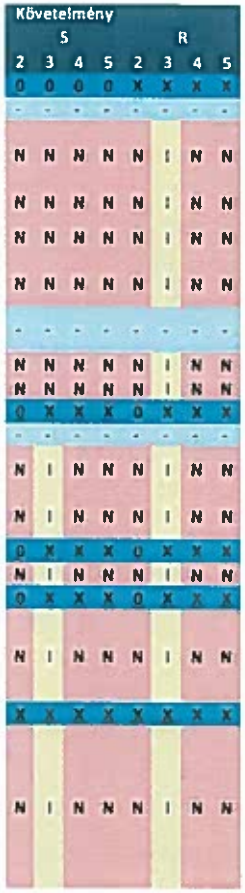
3.2.1.8.	A látogatók ellenőrzése	Megfelelt	Kötelező	0	0	X	X	X
3.2.1.8.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.8.1.1.	meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat;	Igen		N	N	I	N	N
3.2.1.8.1.2.	azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.	Igen		N	N	I	N	N
3.2.1.8.2.	Automatizált látogatói információkezelés	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet automatizált mechanizmusokat alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez, átvizsgálásához.			N	N	N	N	N
3.2.1.9.	Áramellátó berendezések és kábelezés	Nem kötelező	Nem kötelező	0	0	0	X	X
	Az érintett szervezet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.			N	N	N	N	N
3.2.1.9.1.	Tartalék áramellátás	Nem kötelező	Nem kötelező	0	0	0	X	X
	Az érintett szervezet az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.			N	N	N	N	N
3.2.1.9.2.	Hosszútávú tartalék áramellátás a minimálisan elvárt működési képességhez	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet az elsődleges áramforrás kiesése esetén biztosítja a hosszútávú tartalék áramellátást az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.			N	N	N	N	N
3.2.1.10.	Vészkikapcsolás	Nem kötelező	Nem kötelező	0	0	0	X	X
3.2.1.10.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.10.1.1.	lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben;			N	N	N	N	N
3.2.1.10.1.2.	gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről;			N	N	N	N	N
3.2.1.10.1.3.	megakadályozza a jogosulatlan vészkikapcsolást.			N	N	N	N	N
3.2.1.11.	Vészvilágítás	Nem felelt meg	Kötelező	0	0	X	X	X
	Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.	Nem		N	N	I	N	N

3.2.1.12.	Tűzvédelem	Nem felelt meg	Kötelező	0	0	X	X	X
3.2.1.12.1.	Az érintett szervezet az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.	Nem		N	N	I	N	N
3.2.1.12.2.	Automatikus tűzelfojtás	Nem kötelező	Nem kötelező	0	0	0	X	X
	Az érintett szervezet a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít.			N	N	N	N	N
3.2.1.12.3.	Észlelő berendezések, rendszerek	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek.			N	N	N	N	N
3.2.1.12.4.	Tűzelfojtó berendezések, rendszerek	Nem kötelező	Nem kötelező	0	0	0	0	X
	Az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzelfojtó berendezést vagy rendszert alkalmaz, amelynek aktiválásáról automatikusan jelzést kap az érintett szervezet által kijelölt tűzvédelmi felelős.			N	N	N	N	N
3.2.1.13.	Hőmérséklet és páratartalom ellenőrzés	Nem felelt meg	Kötelező	0	0	X	X	X
3.2.1.13.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.13.1.1.	az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat;	Nem		N	N	I	N	N
3.2.1.13.1.2.	az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) figyeli a hőmérséklet és páratartalom szintjét.	Nem		N	N	I	N	N
3.2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	Nem felelt meg	Kötelező	0	0	X	X	X
3.2.1.14.1.	*Az érintett szervezet:*	-		-	-	-	-	-
3.2.1.14.1.1.	védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek;	Nem		N	N	I	N	N
3.2.1.14.1.2.	az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.	Nem		N	N	I	N	N

3.2.1.14.2.	**Automatizált védelem**	Nem kötelező	*Nem kötelező*	0	0	0	0	X		
	Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer közelében megjelenő folyadékszivárgás észlelésére és az érintett szervezet által kijelölt személyek riasztására.			N	N	N	N	N		
3.2.1.15.	**Be- és kiszállítás**	Megfelelt	*Kötelező*	0	0	X	X	X		
	Az érintett szervezet engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.	Igen		N	N	I	N	N		
3.2.1.16.	**Az elektronikus információs rendszer elemeinek elhelyezése**	Nem kötelező	*Nem kötelező*	0	0	0	X	X		
	Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.			N	N	N	N	N		
3.2.1.17.	**Ellenőrzés**	Nem kötelező	*Nem kötelező*	0	0	0	X	X		
	Az érintett szervezet ellenőrzi a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.			N	N	N	N	N		
3.2.1.18.	**Szállítási felügyelet**	Nem kötelező	*Nem kötelező*	0	0	0	0	X		
3.2.1.18.1.	***Az érintett szervezet védi az információt tartalmazó karbantartási eszközt a jogosulatlan elszállítással szemben azzal, hogy:***	-		-	-	-	-	-		
3.2.1.18.1.1.	ellenőrzi, az eszköz nem tartalmaz-e információt;			N	N	N	N	N		
3.2.1.18.1.2.	ha az eszköz tartalmaz információt, azt törli vagy megsemmisíti;			N	N	N	N	N		
3.2.1.18.1.3.	az eszközt a létesítményen belül őrzi;			N	N	N	N	N		
3.2.1.18.1.4.	az ezért felelős személyekkel engedélyezteti az eszköz elszállítását a létesítményből.			N	N	N	N	N		
3.2.1.19.	**Karbantartók**	Megfelelt	*Kötelező*	0	0	X	X	X		
3.2.1.19.1.	***Az érintett szervezet:***	-		-	-	-	-	-		
3.2.1.19.1.1.	kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;	Igen		N	N	I	N	N		
3.2.1.19.1.2.	megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;	Igen		N	N	I	N	N		
3.2.1.19.1.3.	felhatalmazást ad a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.	Igen		N	N	I	N	N		

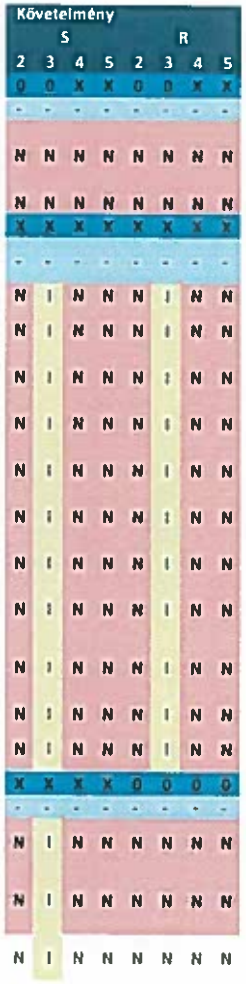
3.2.1.19.2.	**Karbantartás fokozott biztonsági intézkedésekkel**	**Nem kötelező**		**0**	**0**	**0**	**0**	**X**
3.2.1.19.2.1	***Az érintett szervezet***	-		-	-	-	-	-
3.2.1.19.2.1.1.	***a megfelelő biztonsági engedéllyel nem rendelkező karbantartó személyek alkalmazása során:***	-		-	-	-	-	-
3.2.1.19.2.1.1.1.	az ilyen karbantartó személyeket megfelelő hozzáférési jogosultságú, műszakilag képzett belső személyekkel felügyelete alatt tartja az elektronikus információs rendszeren végzett karbantartási és diagnosztikai tevékenységek során,		***Nem kötelező***	**N**	**N**	**N**	**N**	**N**
3.2.1.19.2.1.1.2.	a karbantartási és diagnosztikai tevékenységek megkezdése előtt az elektronikus információs rendszer minden fellelhető információtároló elemét törli, és a nem törölhető adathordozót eltávolítja, vagy fizikailag leválasztja a rendszertől;			**N**	**N**	**N**	**N**	**N**
3.2.1.19.2.1.2.	alternatív biztonsági védelmet alakít ki, ha egy elektronikus információs rendszerelemet nem lehet törölni, eltávolítani vagy a rendszertől leválasztani.			**N**	**N**	**N**	**N**	**N**
3.2.1.19.3.	**Időben történő javítás**	**Nem kötelező**		**0**	**0**	**0**	**X**	**X**
	Az érintett szervezet karbantartási támogatást szerez be a meghatározott elektronikus információs rendszerelemekhez.		***Nem kötelező***	**N**	**N**	**N**	**N**	**N**

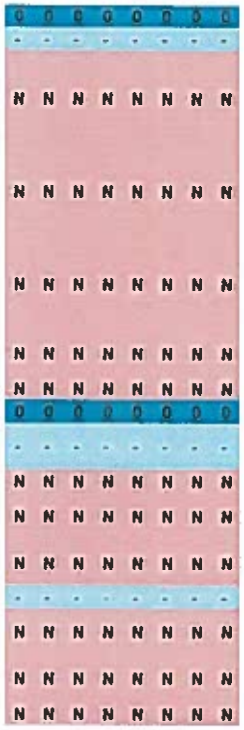
3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Elvárt szint(ek):		3		3					
		Bizalmasság		Sértetlenség		Rendelkezésre állás		B			
3.3.1.	ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	Megfelelt? (i/N)	Ki kell tölteni?	Megfelelt? (i/N)	Ki kell tölteni?	Megfelelt? (i/N)	Ki kell tölteni?	2	3	4	5
3.3.1.1.	Engedélyezés	Nem kötelező		Nem kötelező		Megfelelt		0	0	0	0
3.3.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-
3.3.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;					Igen		N	N	N	N
3.3.1.1.2.	felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;					Igen		N	N	N	N
3.3.1.1.3.	meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket, kijelöli az ezeket betöltő személyeket;		*Nem kötelező*		*Nem kötelező*	Igen	*Kötelező*	N	N	N	N
3.3.1.1.4.	integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.					Igen		N	N	N	N
3.3.1.2.	*Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:*	-		-		-		-	-	-	-
3.3.1.2.1.	emberi, fizikai és logikai erőforrásra;					Igen		N	N	N	N
3.3.1.2.2.	eljárási és védelmi szintre és folyamatra.					Igen		N	N	N	N
3.3.1.3.	Az elektronikus információs rendszer kapcsolódásai	Megfelelt		Megfelelt		Megfelelt		0	X	X	X
3.3.1.3.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-
3.3.1.3.1.1.	szabályozza, és belső engedélyhez kötheti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N
3.3.1.3.1.2.	dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.	Igen		Igen		Igen		N	I	N	N
3.3.1.3.2.	Belső rendszerkapcsolatok	Megfelelt		Megfelelt		Megfelelt		0	X	X	X
	az érintett szervezet belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N
3.3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	Megfelelt		Megfelelt		Megfelelt		0	X	X	X
	Az érintett szervezet a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az informatikai biztonsági szabályzatában szabályrendszert állít fel, és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N
3.3.1.4.	Személybiztonság	Megfelelt		Megfelelt		Megfelelt		X	X	X	X
3.3.1.4.1.	Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N


Követelmény
S
R
2 3 4 5 2 3 4 5

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Bizalmasság		Sértetlenség		Rendelkezésre állás		B			
3.3.2.	TERVEZÉS	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	2	3	4	5
3.3.2.1.	Biztonságtervezési szabályzat	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X
3.3.2.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-
3.3.2.1.1.1.	megfogalmazza, az érintett szervezetre érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési szabályzatot, amely tartalmazza a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését;		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N
3.3.2.1.1.2.	felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;							N	N	N	N
3.3.2.2.	Rendszerbiztonsági terv	Megfelelt		Megfelelt		Megfelelt		X	X	X	X
3.3.2.2.1.	*Az érintett szervezet, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, amely:*	-		-		-		-	-	-	-
3.3.2.2.1.1.	összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.2.	meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.3.	meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.4.	meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.5.	a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.6.	meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N
3.3.2.2.1.7.	gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.8.	belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.9.	frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.10.	elvégzi a szükséges belső egyeztetéseket;	Igen		Igen		Igen		N	I	N	N
3.3.2.2.1.11.	gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.	Igen		Igen		Igen		N	I	N	N
3.3.2.3.	Cselekvési terv	Megfelelt		Megfelelt		Nem kötelező		X	X	X	X
3.3.2.3.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-
3.3.2.3.1.1.	cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;	Igen		Igen		Igen		N	I	N	N
3.3.2.3.1.2.	a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Nem kötelező*	N	I	N	N
3.3.2.3.1.3.	frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.	Igen		Igen		Igen		N	I	N	N

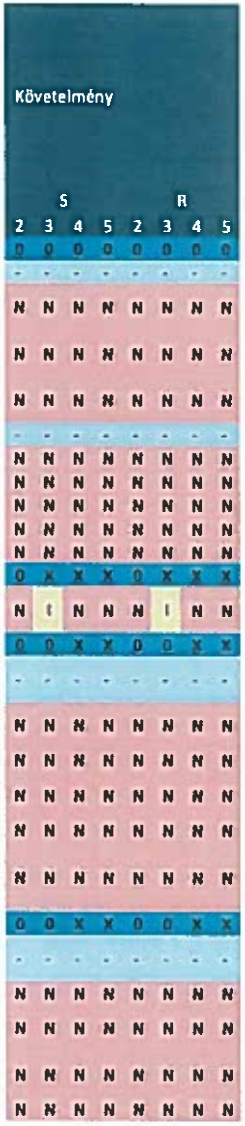
3.3.2.4.	Személyi biztonság	Megfelelt	Kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	X	X	X	X
3.3.2.4.1.	*Az érintett szervezet:*	-		-	-	-		-	-	-	-
3.3.2.4.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;	Igen						N	I	N	N
3.3.2.4.1.2.	az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;	Igen						N	I	N	N
3.3.2.4.1.3.	meghatározott gyakorisággal felülvizsgálja, és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását;	Igen						N	I	N	N
3.3.2.4.1.4.	gondoskodik arról, hogy a 3.3.2.4.1.3. pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a 3.3.2.4.1.2. pont szerinti eljárás megtörténjen;	Igen						N	I	N	N
3.3.2.4.1.5.	meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket.	Igen						N	I	N	N
3.3.2.5.	Információbiztonsági architektúra leírás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	X	X
3.3.2.5.1.	*Az érintett szervezet (ha a hatókörébe tartozik, és ha más dokumentumban nem kerül meghatározásra, vagy azokból nem következik):*	-		-	-	-		-	-	-	-
3.3.2.5.1.1.	elkészíti az elektronikus információs rendszer információbiztonsági architektúra leírását;							N	N	N	N
3.3.2.5.1.2.	az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja, és frissíti az információbiztonsági architektúra leírást;							N	N	N	N
3.3.2.5.1.3.	biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben és a beszerzésekben.							N	N	N	N
3.3.2.5.2.	*Az információbiztonsági architektúra leírás:*	-		-	-	-		-	-	-	-
3.3.2.5.2.1.	összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést;							N	N	N	N
3.3.2.5.2.2.	megfogalmazza, hogy az információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt;							N	N	N	N
3.3.2.5.2.3.	leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.							N	N	N	N

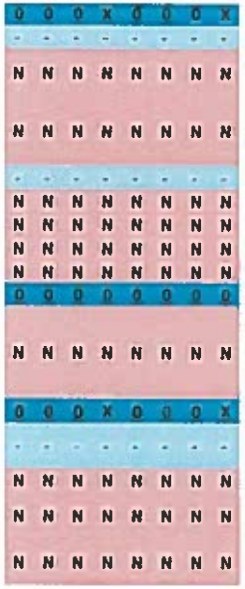

Követelmény
S
R
2 3 4 5 2 3 4 5



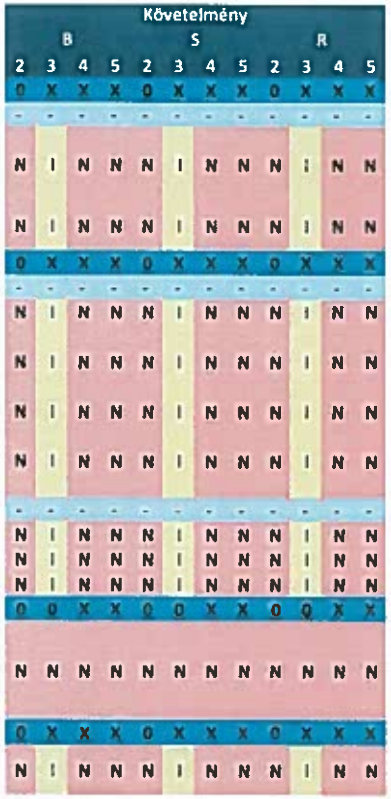
3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Üres cella!									
3.3.3.	RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS										
3.3.3.1.	*Jelen címben meghatározott eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.*	-	-	-	-	-	-				
		Bizalmasság		Sértetlenség		Rendelkezésre állás		B			
		Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	2	3	4	5
3.3.3.2.	A rendszer fejlesztési életciklusa	Megfelelt	Kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	X	X	X	X
3.3.3.2.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-
3.3.3.2.1.1.	elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket;	Igen						N	I	N	N
3.3.3.2.1.2.	a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket;	Igen						N	I	N	N
3.3.3.2.1.3.	meghatározza, és a szervezetre érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.	Igen						N	I	N	N
3.3.3.2.2.	*A rendszer életciklus szakaszai a következők:*	-		-		-		-	-	-	-
3.3.3.2.2.1.	követelmény meghatározás;	Igen						N	I	N	N
3.3.3.2.2.2.	fejlesztés vagy beszerzés;	Igen						N	I	N	N
3.3.3.2.2.3.	megvalósítás vagy értékelés;	Igen						N	I	N	N
3.3.3.2.2.4.	üzemeltetés és fenntartás;	Igen						N	I	N	N
3.3.3.2.2.5.	kivonás (archiválás, megsemmisítés).	Igen						N	I	N	N
3.3.3.3.	Funkciók, portok, protokollok, szolgáltatások	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	0	X	X	X
	Az érintett szervezet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.	Igen		Igen		Igen		N	I	N	N
3.3.3.4.	Fejlesztői változáskövetés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X
3.3.3.4.1.	*Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:*	-		-		-		-	-	-	-
3.3.3.4.1.1.	vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;							N	N	N	N
3.3.3.4.1.2.	dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét;							N	N	N	N
3.3.3.4.1.3.	csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N
3.3.3.4.1.4.	dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait;							N	N	N	N
3.3.3.4.1.5.	kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az érintett szervezet által meghatározott személyeknek.							N	N	N	N
3.3.3.5.	Fejlesztői biztonsági tesztelés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X
3.3.3.5.1.	*Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője:*	-		-		-		-	-	-	-
3.3.3.5.1.1.	készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat;							N	N	N	N
3.3.3.5.1.2.	hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az érintett szervezet által meghatározott lefedettség és mélység mellett;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N
3.3.3.5.1.3.	dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit;							N	N	N	N
3.3.3.5.1.4.	javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.							N	N	N	N

3.3.3.6.	Fejlesztési folyamat, szabványok és eszközök	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X
3.3.3.6.1.	*Az érintett szervezet:*	-	-	-	-	-	-	-
3.3.3.6.1.1.	megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen;				N	N	N	N
3.3.3.6.1.2.	előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N
3.3.3.6.2.	*A dokumentált fejlesztési folyamat:*	-	-	-	-	-	-	-
3.3.3.6.2.1.	kiemelten kezeli a biztonsági követelményeket;				N	N	N	N
3.3.3.6.2.2.	meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket;				N	N	N	N
3.3.3.6.2.3.	dokumentálja a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat;				N	N	N	N
3.3.3.6.2.4.	nyilvántartja a változtatásokat, és biztosítja ezek engedély nélküli megváltoztatás elleni védelmét.				N	N	N	N
3.3.3.7.	Fejlesztői oktatás	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X
	Az érintett szervezet oktatási kötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára, hogy az érintett szervezet által kijelölt személyek - elsősorban adminisztrátorok - és biztonsági felelősök a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N
3.3.3.8.	Fejlesztői biztonsági architektúra és tervezés	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X
3.3.3.8.1.	*Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre, amely:*	-	-	-	-	-	-	-
3.3.3.8.1.1.	illeszkedik a szervezet biztonsági architektúrájához és támogatja azt;				N	N	N	N
3.3.3.8.1.2.	leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között;		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N
3.3.3.8.1.3.	bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.				N	N	N	N

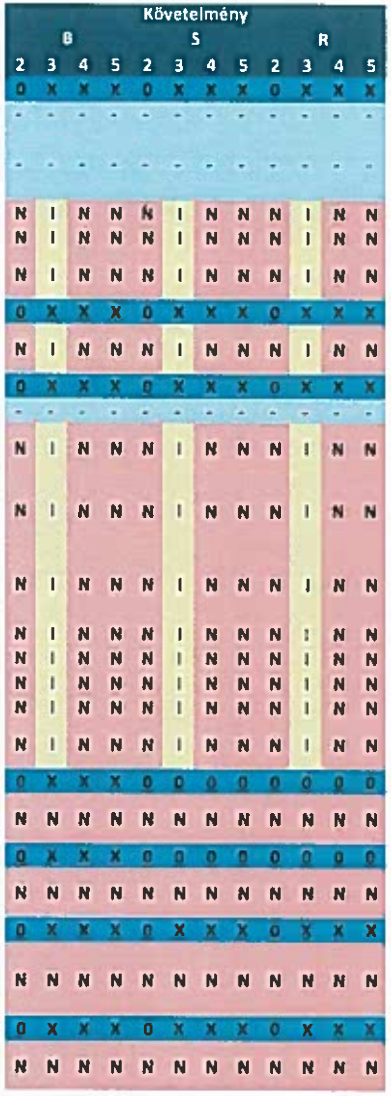

Követelmény
S
R
2 3 4 5 2 3 4 5



3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Elvárásszint:	3	3	3
		Bizalmasság		Sértetlenség		Rendelkezésre állás	
3.3.4.	BIZTONSÁGI ELEMZÉS	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?
3.3.4.1.	Biztonságelemzési eljárásrend	Megfelelt		Megfelelt		Megfelelt	
3.3.4.1.1.	*Az érintett szervezet:*	-		-		-	
3.3.4.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*
3.3.4.1.1.2.	a biztonságértékelési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.	Igen		Igen		Igen	
3.3.4.2.	Biztonsági értékelések	Megfelelt		Megfelelt		Megfelelt	
3.3.4.2.1.	*Az érintett szervezet:*	-		-		-	
3.3.4.2.1.1.	biztonságértékelési tervet készít;	Igen		Igen		Igen	
3.3.4.2.1.2.	meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését;	Igen		Igen		Igen	
3.3.4.2.1.3.	elkészíti a biztonságértékelés eredményét összefoglaló jelentést;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*
3.3.4.2.1.4.	gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.	Igen		Igen		Igen	
3.3.4.2.2.	*A biztonsági értékelés tartalmazza:*	-		-		-	
3.3.4.2.2.1.	az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket;	Igen		Igen		Igen	
3.3.4.2.2.2.	a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket;	Igen		Igen		Igen	
3.3.4.2.2.3.	az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.	Igen		Igen		Igen	
3.3.4.3	Speciális értékelés	Nem kötelező		Nem kötelező		Nem kötelező	
	Az érintett szervezet a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélkül sérülékenységvizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az érintett szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*
3.3.4.4.	A biztonsági teljesítmény mérése	Megfelelt		Megfelelt		Megfelelt	
	Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*


Követelmény
B
S
R
2 3 4 5 2 3 4 5 2 3 4 5

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Hiányt okoló:	1	1	1
3.3.5.	TESZTELÉS, KÉPZÉS ÉS FELÜGYELET	Bizalmasság		Sértetlenség		Rendelkezésre állás	
		Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?
3.3.5.1.	Tesztelési, képzési és felügyeleti eljárások	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező
3.3.5.1.	*Az érintett szervezet:*	-		-		-	
3.3.5.1.1	*ha ez hatókörébe tartozik, megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek:*	-		-		-	
3.3.5.1.1.1.	fejlesztését és fenntartását;	Nem		Nem		Nem	
3.3.5.1.1.2.	folyamatos időbeni végrehajtását;	Nem		Nem		Nem	
3.3.5.1.1.3.	felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.	Nem		Nem		Nem	
3.3.5.2.	A biztonsági teljesítmény mérése	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező
	Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.	Nem		Nem		Nem	
3.3.5.3	Sérülékenység teszt	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező
3.3.5.3.1.	*Az érintett szervezet:*	-		-		-	
3.3.5.3.1.1.	az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik;	Nem		Nem		Nem	
3.3.5.3.1.2.	meghatározott gyakorisággal, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet;	Nem		Nem		Nem	
3.3.5.3.1.3.	a sérülékenység tesztet sérülékenységvizsgálati eszközök és technikák alkalmazásával, vagy külső szervezet bevonásával azon elektronikus információs rendszerek tekintetében végzi el, amelyek az érintett szervezet felügyelete, irányítása alatt állnak;	Nem		Nem		Nem	
3.3.5.3.1.4.	kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;	Nem		Nem		Nem	
3.3.5.3.1.5.	végrehajtja az ellenőrzési listákat és tesztelési eljárásokat;	Nem		Nem		Nem	
3.3.5.3.1.6.	felméri a sérülékenység lehetséges hatásait;	Nem		Nem		Nem	
3.3.5.3.1.7.	elemzi a sérülékenység teszt eredményét;	Nem		Nem		Nem	
3.3.5.3.1.8.	megosztja a sérülékenység teszt eredményét a szervezet által meghatározott személyekkel és szerepkörökkel.	Nem		Nem		Nem	
3.3.5.3.2.	Frissítési képesség	Nem felelt meg	Kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező
	Az érintett szervezet olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.	Nem					
3.3.5.3.3.	Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően	Nem felelt meg	Kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező
	Az érintett szervezet az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizálja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.	Nem					
3.3.5.3.4.	Privilegizált hozzáférés	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező
	Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít az érintett szervezet által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.	Nem		Nem		Nem	
3.3.5.3.5.	Felfedhető információk	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező	Nem felelt meg	Kötelező
	Az érintett szervezet meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.	Nem		Nem		Nem	


Követelmény
B
S
R
2 3 4 5 2 3 4 5 2 3 4 5

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Bizalmasság		Sértetlenség		Rendelkezésre állás		Követelmény											
3.3.6.	KONFIGURÁCIÓKEZELÉS	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	B				S				R			
								2	3	4	5	2	3	4	5	2	3	4	5
3.3.6.1.	Konfigurációkezelési eljárásrend	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.6.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.1.1.2.	a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.2.	Alapkonfiguráció	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.6.2.1.	Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.2.2.	Áttekintések és frissítések	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.2.3.	Korábbi konfigurációk megőrzése	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját, és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.2.4.	Magas kockázatú területek konfigurálása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.6.2.4.1.	Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.2.4.2.	Megfelelő biztonsági eljárásokat kell alkalmazni a 3.3.6.2.4.1. pont szerinti eszköz belső használatba vonásakor.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.2.5.	Automatikus támogatás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Automatikus mechanizmusokat kell alkalmazni az elektronikus információs rendszer naprakész, teljes, pontos, és állandóan rendelkezésre álló alapkonfigurációjának a karbantartására.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.3.	A konfigurációváltozások felügyelete (változáskezelés)	Megfelelt		Megfelelt		Megfelelt		0	X	X	X	0	X	X	X	0	X	X	X
3.3.6.3.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.3.1.1.	meghatározza a változáskezelési felügyelet alá eső változástípusokat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.1.2.	meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.);	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.1.3.	megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.1.4.	dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.1.5.	megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.1.6.	visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.1.7.	auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.3.2.	Előzetes tesztelés és megerősítés	Nem kötelező		Nem kötelező		Megfelelt		0	0	X	X	0	0	X	X	0	X	X	X
	A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.		Nem kötelező		Nem kötelező	Igen	Kötelező	N	N	N	N	N	N	N	N	N	I	N	N
3.3.6.3.3.	Automatikus támogatás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
3.3.6.3.3.1.	*Automatikus mechanizmusokat kell alkalmazni:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.3.3.1.1.	az elektronikus információs rendszerben javasolt változtatások dokumentálására;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.3.3.1.2.	a jóváhagyásra jogosultak értesítésére;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.3.3.1.3.	a késedelmes jóváhagyások kiemelésére;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.3.3.1.4.	a még nem jóváhagyott változások végrehajtásának a megakadályozására;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.3.3.1.5.	az elektronikus információs rendszerben végrehajtott változások teljes dokumentálására;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.3.3.1.6.	a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.4.	Biztonsági hatásvizsgálat	Megfelelt		Megfelelt		Megfelelt		0	X	X	X	0	X	X	X	0	X	X	X
3.3.6.4.1.	Az érintett szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.4.2.	Elkülönített tesztkörnyezet	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X

	Az érintett szervezet a változtatásokat éles rendszerben történő megvalósításuk előtt egy elkülönített tesztkörnyezetben vizsgálja, hibákat, sebezhetőségeket, kompatibilitási problémákat és szándékos károkozásra utaló jeleket keresve.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.5.	A változtatásokra vonatkozó hozzáférés korlátozások	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	O	O	O	X	X	O	O	O	O
3.3.6.5.1.	Az érintett szervezet belső szabályozásában meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.5.2.	Automatikus támogatás	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	O	O	O	O	X	O	O	O	O
	Az érintett szervezet az elektronikus információs rendszerben automatikus mechanizmusokat alkalmaz a hozzáférési korlátozások érdekében, az ezzel kapcsolatos tevékenység naplózására.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.5.3.	Felülvizsgálat	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	O	O	O	O	X	O	O	O	O
	Az érintett szervezet rendszeresen felülvizsgálja az elektronikus információs rendszer változtatásait annak megállapítására, hogy történt-e jogosulatlan változtatás.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.5.4.	Aláírt elemek	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	O	O	O	O	X	O	O	O	O
	A szervezet által meghatározott szoftver- és az úgynevezett firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva ismert és jóváhagyott tanúsítvány alkalmazásával.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.6.	Konfigurációs beállítások	Megfelelő	Kötelező	Megfelelő	Kötelező	Megfelelő	Kötelező	O	X	X	X	O	X	X	X	O	X	X	X
3.3.6.6.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.6.1.1.	meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon - a „szükséges minimum” elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.6.1.2.	elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.6.1.3.	a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.6.1.4.	figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett szervezet belső szabályzataival és eljárásaival összhangban.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.6.2.	Automatikus támogatás	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az érintett szervezet automatikus mechanizmusokat alkalmaz a konfigurációs beállítások központi kezelésére, alkalmazására és ellenőrzésére.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.6.3.	Reagálás jogosulatlan változásokra	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az érintett szervezet meghatározott intézkedéseket vezet be a meghatározott konfigurációs beállítások jogosulatlan változtatásai esetén.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.7.	Legszűkebb funkcionalitás	Megfelelő	Kötelező	Megfelelő	Kötelező	Megfelelő	Kötelező	O	X	X	X	O	X	X	X	O	X	X	X
3.3.6.7.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.7.1.1.	az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.7.1.2.	meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N

3.3.6.7.2.	Rendszeres felülvizsgálat	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.6.7.2.1.	Az érintett szervezet meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.7.2.2.	Az érintett szervezetnek a szoftver használatra meghatározott szabályzatainak, vagy a szoftver használatára vonatkozó feltételeinek és kikötéseinek megfelelően az elektronikus információs rendszer megakadályozza a tiltott programok futtatását.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.7.3.	Nem futtatható szoftverek	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját és megtiltja ezek futtatását.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.7.4.	Futtatható szoftverek	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben jogosultan futtatható (engedélyezett, úgynevezett fehérlistás) szoftverek listáját és engedélyezi ezek futtatását, az ettől eltérő szoftver futtatását egyedi engedélyhez köti.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.8.	Elektronikus információs rendszerelem leltár	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.6.8.1.	*Az érintett szervezet:*	-	Kötelező	-	Kötelező	-	Kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.8.1.1.	leltárt készít az elektronikus információs rendszer elemeiről;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.8.1.2.	meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.8.1.3.	*gondoskodik arról, hogy a leltár:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.8.1.3.1.	pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.8.1.3.2.	az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.8.1.3.3.	legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.8.2.	Frissítés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet az elektronikus információs rendszerelem leltárt frissíti az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.8.3.	Jogosulatlan elemek automatikus észlelése	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	X	X
3.3.6.8.3.1.	Automatizált mechanizmusok biztosítják, hogy a szervezet által meghatározott gyakorisággal a jogosulatlan hardver-, szoftver- és firmware elemek észlelése megtörténjen.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.8.3.2.	A jogosulatlan elemek észlelése esetén le kell tiltani az ilyen elemek általi hálózati hozzáférést; el kell őket különíteni, és értesíteni kell az illetékes személyeket.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.8.4.	Duplikálás elleni védelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	X	X
	Az érintett szervezet ellenőrzi, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.8.5.	Automatikus [illegible]	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet automatikus mechanizmusokat alkalmaz az elektronikus információs rendszerelem leltár naprakész, teljes, pontos, és állandóan rendelkezésre álló kezelésének támogatására.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.8.6.	Naplózás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszerelem leltárhoz csatolni kell az egyes elemek adminisztrálásáért felelős személyek nevét, pozícióját vagy szerepkörét.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.9.	Konfigurációkezelési terv	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.6.9.1.	*Az érintett szervezet:*	-	Nem kötelező	-	Nem kötelező	-	Nem kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.9.1.1.	kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.9.1.2.	bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfigurációelemek konfigurációjának kezelésére;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.9.1.3.	meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.6.9.1.4.	védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.6.10.	A szoftverhasználat korlátozásai	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.6.10.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.10.1.1.	kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.10.1.2.	a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.10.1.3.	ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.11.	A felhasználó által telepített szoftverek	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.6.11.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.6.11.1.1.	megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségét;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.11.1.2.	érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.6.11.1.3.	meghatározott gyakorisággal ellenőrzi a szabályok betartását.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Bizalmasság		Sértetlenség		Rendelkezésre állás		Követelmény											
3.3.7.	KARBANTARTÁS	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	B				S				R			
								2	3	4	5	2	3	4	5	2	3	4	5
3.3.7.1.	Rendszer karbantartási eljárásrend	Nem kötelező	Nem kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	O	O	O	O	X	X	X	X	X	X	X	X
3.3.7.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.7.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;		Nem kötelező	Igen	Kötelező	Igen	Kötelező	N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.1.1.2.	a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.			Igen		Igen		N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.	Rendszeres karbantartás	Nem kötelező	Nem kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	O	O	O	O	X	X	X	X	X	X	X	X
3.3.7.2.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.7.2.1.1.	a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően;		Nem kötelező	Igen	Kötelező	Igen	Kötelező	N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.1.2.	jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;			Igen		Igen		N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.1.3.	az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a szervezeti létesítményből;			Igen		Igen		N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.1.4.	az elszállítás előtt minden adatot és információt - mentést követően - töröl a berendezésről;			Igen		Igen		N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.1.5.	ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;			Igen		Igen		N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.1.6.	csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.			Igen		Igen		N	N	N	N	N	I	N	N	N	I	N	N
3.3.7.2.2.	Automatikus támogatás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	O	O	O	O	X	X	O	O	X	X
3.3.7.2.2.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.7.2.2.1.1.	automatizált mechanizmusokat alkalmaz a karbantartások és javítások ütemezésére, lefolytatására és dokumentálására;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.2.2.1.2.	naprakész, pontos és teljes nyilvántartást készít minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási akcióról.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.3.	Karbantartási eszközök	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	O	O	O	O	X	X	O	O	X	X
3.3.7.3.1.	Az érintett szervezet jóváhagyja, nyilvántartja és ellenőrzi az elektronikus információs rendszer karbantartási eszközeit.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.3.2.	Adathordozó ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	O	O	O	O	X	X	O	O	X	X
	Az érintett szervezet ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.	Távoli karbantartás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	X	X	O	O	X	X	O	O	X	X
3.3.7.4.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.7.4.1.1.	jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.1.2.	akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.1.3.	hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.1.4.	nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.1.5.	lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.7.4.2.	Dokumentálás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet az elektronikus információs rendszer rendszerbiztonsági tervében dokumentálja a távoli karbantartási és diagnosztikai kapcsolatok létrehozására és használatára vonatkozó szabályokat és eljárásokat.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.3.	Összehasonlítható biztonság	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
3.3.7.4.3.1.	Az érintett szervezet megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan elektronikus információs rendszerből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a szervizelt rendszer biztonsági képességekkel.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.3.2.	Ha a 3.3.7.4.3.1. pont szerinti eljárás nem biztosított, a szervizelendő elemet el kell távolítani az elektronikus információs rendszerből, és a távoli karbantartási és diagnosztikai szervizelést megelőzően minden információt törölni kell az érintett rendszerelemről.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.7.4.3.3.	Ha a 3.3.7.4.3.1., vagy a 3.3.7.4.3.2. pont szerinti eljárást nem lehet lefolytatni, a szervizelés végrehajtását követően át kell vizsgálni az elemet a lehetséges kártékony szoftverek miatt, mielőtt visszakapcsolják az elektronikus információs rendszerhez.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Kivárt oszlop	3		4		5	Követelmény											
		Bizalmasság		Sértetlenség		Rendelkezésre állás		B				S				R			
3.3.8.	ADATHORDOZÓK VÉDELME	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	2	3	4	5	2	3	4	5	2	3	4	5
3.3.8.1.	Adathordozók védelmére vonatkozó eljárásrend	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.8.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.8.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az adathordozók védelmére vonatkozó eljárásrendet, mely az adathordozókra vonatkozó védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.8.1.1.2.	az adathordozók védelmére vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az adathordozók védelmére vonatkozó eljárásrendet.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.8.2.	Hozzáférés az adathordozókhoz	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
	Az érintett szervezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.8.3.	Adathordozók címkézése	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	0	0	0	0	0	0
	Az érintett szervezet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.4.	Adathordozók tárolása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	0	0	0	0	0	0
3.3.8.4.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.8.4.1.1.	fizikailag ellenőrzi és biztonságosan tárolja az adathordozókat, az arra engedélyezett, vagy kijelölt helyen;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.4.1.2.	védi az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.5.	Adathordozók szállítása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.8.5.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.8.5.1.1.	meghatározott biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.5.1.2.	biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.5.1.3.	dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.5.1.4.	korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.5.2.	Kriptográfiai védelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.6.	Adathordozók törlése	Megfelelt		Nem kötelező		Nem kötelező		X	X	X	X	0	0	0	0	0	0	0	0
3.3.8.6.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.8.6.1.1.	a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt;	Igen	Kötelező		Nem kötelező		Nem kötelező	N	I	N	N	N	N	N	N	N	N	N	N
3.3.8.6.1.2.	a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.	Igen						N	I	N	N	N	N	N	N	N	N	N	N

3.3.8.6.2.	Ellenőrzés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	0	0	0	0	0
	Az érintett szervezet felülvizsgálja, jóváhagyja, nyomon követi, dokumentálja és ellenőrzi az adathordozók törlésével és megsemmisítésével kapcsolatos tevékenységeket.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.6.3.	Tesztelés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	0	0	0	0	0
	A törlésre alkalmazott eszközöket és eljárásokat meghatározott gyakorisággal tesztelni kell.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.6.4.	Törlés megsemmisítés nélkül	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	0	0	0	0	0
	Nem romboló törlési technikák alkalmazhatók a meghatározott hordozható tárolóeszközökre, mielőtt ilyen eszközöket az elektronikus információs rendszerhez csatolnak.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.8.7.	Adathordozók használata	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.8.7.1.	Az érintett szervezet engedélyezi, korlátozza, vagy tiltja egyes, vagy bármely adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N	N	I	N	N	N	I	N	N
3.3.8.7.2.	Ismeretlen tulajdonos	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK							Követelmény											
		Bizalmasság		Sértetlenség		Rendelkezésre állás		B				S				R			
3.3.9.	AZONOSÍTÁS ÉS HITELESÍTÉS	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	2	3	4	5	2	3	4	5	2	3	4	5
3.3.9.1.	Azonosítási és hitelesítési eljárásrend	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.9.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.9.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.1.1.2.	az azonosítási és hitelesítésre vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az azonosítási és hitelesítésre vonatkozó eljárásrendet.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.2.	Azonosítás és hitelesítés	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.9.2.1.	Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, a felhasználók által végzett tevékenységet.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.2.2.	Hálózati hozzáférés privilegizált fiókokhoz	Megfelelő		Nem kötelező		Nem kötelező		0	X	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.	Igen	Kötelező		Nem kötelező		Nem kötelező	N	I	N	N	N	N	N	N	N	N	N	N
3.3.9.2.3.	Hálózati hozzáférés nem privilegizált fiókokhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.2.4.	Helyi hozzáférés privilegizált fiókokhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.2.5.	Visszajátszás-védelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.2.6.	Távoli hozzáférés - külön eszköz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.2.7.	Helyi hozzáférés nem privilegizált fiókokhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.2.8.	Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.3.	Eszközök azonosítása és hitelesítése	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi, vagy távoli hálózati kapcsolatot létesítene velük.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.4.	Azonosító kezelés	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.9.4.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.9.4.1.1.	az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.4.1.2.	hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.4.1.3.	meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.4.1.4.	meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N

3.3.9.5.	A hitelesítésre szolgáló eszközök kezelése	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.9.5.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.9.5.1.1.	ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.2.	meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.3.	biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.4.	dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.5.	megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.6.	meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.7.	a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.8.	megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.9.	megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.1.10.	lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.5.2.	Jelszó (tudás) alapú hitelesítés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.9.5.2.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.9.5.2.1.1.	a jelszóra a következő elvárásokat érvényesíti: kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.2.1.2.	meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.2.1.3.	a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást) és nem továbbítja;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.2.1.4.	a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.3.	Birtoklás alapú hitelesítés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.9.5.3.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.9.5.3.1.1.	az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az érintett szervezet által meghatározott minőségi követelményeknek, vagy							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.3.1.2.	*az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.9.5.3.1.2.1.	ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.3.1.2.2.	kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.3.1.2.3.	összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.3.1.2.4.	megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.4.	Tulajdonság alapú hitelesítés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet a felhasználó egyedi (biometrikus) azonosítást lehetővé tevő tulajdonságai alapján végzi el az azonosítást (pl.: ujjlenyomat, retina letapogatás, és más hasonló).		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N

3.3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	X	X	X	X	X	X	X	X	X	X	X	X
	Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.7.	Hitelesítés kriptográfiai modul esetén	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	O	X	X	X	O	X	X	X	O	X	X	X
	Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.8.	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	X	X	X	X	X	X	X	X	X	X	X	X
3.3.9.8.1.	Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett szervezeten kívüli felhasználókat, és tevékenységüket.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.9.8.2.	Hitelesítésszolgáltatók tanúsítványának elfogadása	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	O	X	X	X	X	X	X	X	X	X	X	X
	Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Bizalmasság		Sértetlenség		Rendelkezésre állás		Követelmény											
3.3.10.	HOZZÁFÉRÉS ELLENŐRZÉSE	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	B				S				R			
								2	3	4	5	2	3	4	5	2	3	4	5
3.3.10.1.	Hozzáférés ellenőrzési eljárásrend	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.10.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.1.1.2.	a hozzáférés védelmére vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférések védelmére vonatkozó eljárásrendet.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.	Felhasználói fiókok kezelése	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.10.2.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.2.1.1.	meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait, és ezek típusait;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.2.	kijelöli a felhasználói fiókok fiókkezelőit;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.3.	kialakítja a csoport- és szerepkör tagsági feltételeket;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.4.	meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.5.	létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.6.	ellenőrzi a felhasználói fiókok használatát;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.7.	*értesíti a fiókkezelőket, ha:*	-	Kötelező	-	Kötelező	-	Kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.2.1.7.1.	a felhasználói fiókokra már nincsen szükség,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.7.2.	a felhasználók kiléptek vagy áthelyezésre kerültek,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.7.3.	az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.8.	*feljogosít az elektronikus információs rendszerhez való hozzáférésre:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.2.1.8.1.	az érvényes hozzáférési engedély,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.8.2.	a tervezett rendszerhasználat,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.8.3.	az alapfeladatok és funkcióik alapján;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.9.	meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.1.10.	kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök vagy adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.2.2.	Automatikus kezelés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer fiókjainak kezeléséhez.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.2.3.	Ideiglenes fiókok eltávolítása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja, vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat, vagy egyes kijelölt felhasználói fiók típusokat.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.2.4.	Inaktív fiókok letiltása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat meghatározott időtartam letelte után.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.2.5.	Automatikus naplózás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N

3.3.10.2.6.	Kiléptetés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Meghatározott időtartamú várható inaktivitás, vagy egyéb előre meghatározott esetekben ki kell léptetni a felhasználót.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.2.7.	Szokatlan használat	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Figyelni kell az elektronikus információs rendszer fiókjait az érintett szervezet által meghatározott szokatlan használat szempontjából, és meghatározott személyeknek vagy szerepköröknek jelenteni kell azt.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.2.8.	Letiltás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Azonnal le kell tiltani a kockázatot jelentő felhasználók fiókjait.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.3.	Hozzáférés ellenőrzés érvényesítése	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
	Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.4.	Információáramlás ellenőrzés érvényesítése	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az érintett szervezet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.5.	A felelősségek szétválasztása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.10.5.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.5.1.1.	szétválasztja az egyéni felelősségeket;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.5.1.2.	dokumentálja az egyéni felelősségek szétválasztását;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.5.1.3.	meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.	Legkisebb jogosultság elve	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.10.6.1.	Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.4.	Privilegizált fiókok	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.5.	Privilegizált funkciók használatának naplózása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.6.	Privilegizált funkciók tiltása nem privilegizált felhasználóknak	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.6.7.	Hálózati hozzáférés a privilegizált parancsokhoz	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X

	A meghatározott privilegizált parancsok hálózaton keresztüli elérését csak meghatározott üzemeltetési szükséghelyzetben lehet engedélyezni, és az ilyen hozzáférések indoklását dokumentálni kell a rendszerbiztonsági tervben. Privilegizált parancsok csak meghatározott munkaállomásokról, terminálokról, szegmensekről és IP címekről adhatóak ki, mely munkaállomások/terminálok helyiségei fizikai hozzáférés szempontjából normáltól eltérő szintű besorolást kapnak.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.7.	Sikertelen bejelentkezési kísérletek	Megfelelő	Kötelező	Megfelelő	Kötelező	Megfelelő	Kötelező	0	X	X	X	0	X	X	X	0	X	X	X
3.3.10.7.1.	*Az elektronikus információs rendszer:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.7.1.1.	az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belüli egymást követő sikertelen bejelentkezési kísérletekre;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.7.1.2.	amennyiben a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.	A rendszerhasználat jelzése	Megfelelő	Kötelező	Megfelelő	Kötelező	Megfelelő	Kötelező	0	X	X	X	0	X	X	X	0	X	X	X
3.3.10.8.1.	*Az érintett szervezet az elektronikus információs rendszer felhasználásával:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.8.1.1.	*az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.8.1.1.1.	a felhasználó az érintett szervezet elektronikus információs rendszerét használja;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.1.1.2.	a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.1.1.3.	a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.1.1.4.	a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.2.	Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.3.	*Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.8.3.1.	kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.3.2.	amennyiben felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.8.3.3.	leírást biztosít a rendszer engedélyezett felhasználásáról.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.9.	Egyidejű munkaszakasz kezelés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.10.	A munkaszakasz zárolása	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
3.3.10.10.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.10.1.1.	meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.10.1.2.	megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.10.2.	Képernyőtakarás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.11.	A munkaszakasz lezárása	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	X	X	X	X	X	X	X	X	X	X	X	X
3.3.10.12.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.12.1.1.	kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.12.1.2.	dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.13.	Távoli hozzáférés	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	0	X	X	X	0	X	X	X	0	X	X	X
3.3.10.13.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.13.1.1.	kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.13.1.2.	engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.13.2.	Ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.13.3.	Titkosítás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.13.4.	Hozzáférés ellenőrzési pontok	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányitani az elektronikus információs rendszerben.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.13.5.	Privilegizált parancsok elérése	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
3.3.10.13.5.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.13.5.1.1.	privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.13.5.1.2.	dokumentálja és indokolja a 3.3.10.13.5.1.1. pont szerinti hozzáféréseket a rendszerbiztonsági tervben.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.14.	Vezeték nélküli hozzáférés	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	0	X	X	X	0	X	X	X	0	X	X	X
3.3.10.14.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.14.1.1.	belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.14.1.2.	engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.14.2.	Hitelesítés és titkosítás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet az elektronikus információs rendszerben titkosítással és a felhasználók, vagy eszközök hitelesítésével védi a vezeték nélküli hozzáférést.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.14.3.	Felhasználói konfigurálás tiltása	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.14.4.	Antennák	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet olyan karakterisztikájú és teljesítményszintű antennákat és árnyékolási megoldásokat üzemeltet, vagy egyéb technikákat alkalmaz, amelyekkel csökkenti az érintett szervezet fizikai védelmi határain kívül a jelek észlelésének a valószínűségét.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.10.15.	Mobil eszközök hozzáférés ellenőrzése	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	0	X	X	X	0	X	X	X	0	X	X	X
3.3.10.15.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.15.1.1.	belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.15.1.2.	engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.15.2.	Titkosítás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	0	0
	Az érintett szervezet teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.16.	Külső elektronikus információs rendszerek használata	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	X	X	X	X	X	X	X	X	X	X	X	X
3.3.10.16.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.16.1.1.	meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.16.1.2.	meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az érintett szervezet által ellenőrzött információkat.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.16.2.	Korlátozott használat	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
3.3.10.16.2.1.	*Az érintett szervezet csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az az általa ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.16.2.1.1.	előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.16.2.1.2.	jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.16.3.	Hordozható adattároló eszközök	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	Az érintett szervezet korlátozza, vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező személyek számára.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.17.	Információmegosztás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	0	0	0	0	0	0
3.3.10.17.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.17.1.1.	elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.17.1.2.	automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.10.18.	Nyilvánosan elérhető tartalom	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	X	X	X	X	X	X	X	X	X	X	X	X
3.3.10.18.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.10.18.1.1.	kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett szervezettel kapcsolatos bármely információ közzétételére;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.18.1.2.	a 3.3.10.18.1.1. pont szerinti kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.18.1.3.	közzététel előtt átvizsgálja a javasolt tartalmat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.10.18.1.4.	meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Elvárt szint:	0	1	2																							
3.3.11.	RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	Megfelelt? (I/N)																										
3.3.11.1.	*Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert az érintett szervezet üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni a 3.3.11. pontban és alpontjaiban foglaltakat, és azokat a szolgáltatónak kell biztosítania.*		-	-	-	-	-																					
			Bizalmasság		Sértetlenség		Rendelkezésre állás		Követelmény																			
									B					S						R							
			Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	2	3	4	5	2	3	4	5	2	3	4	5	2	3	4	5				
3.3.11.2.	Rendszer- és információsértetlenségre vonatkozó eljárásrend	Nem kötelező	*Nem kötelező*	Megfelelt	*Kötelező*	Nem kötelező	*Nem kötelező*	0	0	0	0	X	X	X	X	0	0	0	0								
3.3.11.2.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-	-								
3.3.11.2.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, rendszer- és információsértetlenségre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;			Igen					N	N	N	N	I	I	N	N	N	N	N	N								
3.3.11.2.1.2.	a rendszer- és információsértetlenségre vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer- és információsértetlenségre vonatkozó eljárásrendet.			Igen					N	N	N	N	I	I	N	N	N	N	N	N								
3.3.11.3.	Hibajavítás	Nem kötelező	*Nem kötelező*	Megfelelt	*Kötelező*	Nem kötelező	*Nem kötelező*	0	0	0	0	X	X	X	X	0	0	0	0								
3.3.11.3.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-	-								
3.3.11.3.1.1.	azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit;			Igen					N	N	N	N	I	I	N	N	N	N	N	N								
3.3.11.3.1.2.	telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett szervezet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából;			Igen					N	N	N	N	I	I	N	N	N	N	N	N								
3.3.11.3.1.3.	a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti;			Igen					N	N	N	N	I	I	N	N	N	N	N	N								
3.3.11.3.1.4.	beépíti a hibajavítást a konfigurációkezelési folyamatba.			Igen					N	N	N	N	I	I	N	N	N	N	N	N								
3.3.11.3.2.	Automatizált hibajavítási állapot	Nem kötelező	*Nem kötelező*	Nem kötelező	*Nem kötelező*	Nem kötelező	*Nem kötelező*	0	0	0	0	0	0	X	X	0	0	0	0								
	Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemei hibajavítási állapotának meghatározására.								N	N	N	N	N	N	N	N	N	N	N	N								
3.3.11.3.3.	Központi kezelés	Nem kötelező	*Nem kötelező*	Nem kötelező	*Nem kötelező*	Nem kötelező	*Nem kötelező*	0	0	0	0	0	0	0	0	0	0	0	0								
	Az érintett szervezet központilag kezeli a hibajavítás folyamatát.								N	N	N	N	N	N	N	N	N	N	N	N								
3.3.11.4.	Kártékony kódok elleni védelem	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	Megfelelt	*Kötelező*	X	X	X	X	X	X	X	X	X	X	X	X								
3.3.11.4.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-	-								
3.3.11.4.1.1.	az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N								
3.3.11.4.1.2.	frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódírtó rendszeréhez frissítések jelennek meg;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N								
3.3.11.4.1.3.	*konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-	-								
3.3.11.4.1.3.1.	rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési, vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N								
3.3.11.4.1.3.2.	a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt; és riassza a rendszeradminisztrátort, és az érintett szervezet által meghatározott további személy(eke)t;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N								
3.3.11.4.1.4.	ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N								
3.3.11.4.2.	Központi kezelés	Nem kötelező	*Nem kötelező*	Nem kötelező	*Nem kötelező*	Nem kötelező	*Nem kötelező*	0	0	X	X	0	0	X	X	0	0	X	X								
	Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.							N	N	N	N	N	N	N	N	N	N	N	N								

3.3.11.4.3.	Automatikus frissítés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.5.	Az elektronikus információs rendszer felügyelete	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.11.5.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.11.5.1.1.	felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.5.1.2.	azonosítja az elektronikus információs rendszer jogosulatlan használatát;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.5.1.3.	felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére; és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.5.1.4.	védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.5.1.5.	erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.5.1.6.	meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.5.2.	Automatizálás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.5.3.	Felügyelet	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.5.4.	Riasztás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.6.	Biztonsági riasztások és tájékoztatások	Megfelelt		Megfelelt		Megfelelt		0	X	X	X	0	X	X	X	0	X	X	X
3.3.11.6.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.11.6.1.1.	folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.6.1.2.	folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;	Igen	*Kötelező*	Igen	*Kötelező*	Igen	*Kötelező*	N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.6.1.3.	szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.6.1.4.	a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.6.1.5.	kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.6.1.6.	megfelelő ellenintézkedéseket és válaszlépéseket tesz.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.11.6.2.	Automatikus riasztások	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Mechanizmusokat kell kialakítani a biztonsági riasztások és figyelmeztetések szervezeten belüli elérhetőségének biztosítására.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N

3.3.11.7.	A biztonsági funkcionalitás ellenőrzése	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	O
3.3.11.7.1.	*Az elektronikus információs rendszer:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.11.7.1.1.	ellenőrzi a beállított biztonsági funkciókat az ellenőrzésre jogosult felhasználó utasítására, vagy időszakosan;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.7.1.2.	értesítést küld az érintett szervezet által meghatározott személyeknek vagy szerepköröknek, ha az ellenőrzés hibát tár fel;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.7.1.3.	rendellenesség észlelése esetén leállítja a rendszert, az érintett szerv által alkalmazott döntése szerint újraindítja a rendszert, vagy egyéb ellenintézkedést valósít meg.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.8.	Szoftver- és információsértetlenség	Nem kötelező		Nem kötelező		Nem kötelező		O	O	X	X	O	O	X	X	O	O	X	X
3.3.11.8.1.	Az érintett szervezet sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.8.2.	Sértetlenség ellenőrzés	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az elektronikus információs rendszer sértetlenség ellenőrzést hajt végre a meghatározott szoftverekre és információkra, a rendszer újraindításakor, vagy biztonsági esemény bekövetkezését követően, vagy meghatározott gyakorisággal.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.8.3.	Észlelés és reagálás	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az érintett szervezet beépíti az elektronikus információs rendszer jogosulatlan változtatásainak észlelését a biztonsági eseményekre reagáló eljárásaiba.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.8.4.	Automatikus értesítés	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az érintett szervezet automatizált eszközöket alkalmaz a meghatározott személyek vagy szerepkörök értesítésére, ha a sértetlenség ellenőrzés rendellenességet tár fel.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.8.5.	Automatikus reagálás	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az elektronikus információs rendszer automatikusan leállítja, vagy újraindítja a rendszert, vagy egyéb intézkedést valósít meg, ha a sértetlenség ellenőrzés rendellenességet tár fel.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.8.6.	Végrehajtható kód	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	X	O	O	O	X	O	O	O	X
	Az elektronikus információs rendszer megtiltja az olyan bináris vagy gépi kód használatát, amely nem ellenőrzött forrásból származik, vagy amelynek forráskódjával nem rendelkezik.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.9.	Kéretlen üzenetek elleni védelem	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	O	O	O	X	X	O	O	O	O
3.3.11.9.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.11.9.1.1.	kéretlen üzenetek - úgynevezett levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.9.1.2.	új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.9.2.	Központi kezelés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	O	O	O	O	X	X	O	O	O	O
	Az érintett szervezet központi beállításokkal irányítja a levélszemét elleni védelmet.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.9.3.	Frissítés	Nem kötelező		Nem kötelező		Nem kötelező		O	O	O	O	O	O	X	X	O	O	O	O
	Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.10.	Bemeneti információ ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	O	O	O	O	O	O	X	X	O	O	O	O
	Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.11.11.	Hibakezelés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	X	X	0	0	0	0
3.3.11.11.1.	*Az elektronikus információs rendszer:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.11.11.1.1.	hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak;		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.11.1.2.	a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.11.12.	A kimeneti információ kezelése és megőrzése	Megfelelt		Megfelelt		Nem kötelező		X	X	X	X	X	X	X	X	0	0	0	0
	Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.	Igen	*Kötelező*	Igen	*Kötelező*		*Nem kötelező*	N	I	N	N	N	I	N	N	N	N	N	N
3.3.11.13.	Memóriavédelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától.		*Nem kötelező*		*Nem kötelező*		*Nem kötelező*	N	N	N	N	N	N	N	N	N	N	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK	Előző oszlop:	1		2		3		Követelmény											
		Bizalmasság		Sértetlenség		Rendelkezésre állás			B				S				R			
3.3.12.	NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?		2	3	4	5	2	3	4	5	2	3	4	5
3.3.12.1.	Naplózási eljárásrend	Megfelelt		Megfelelt		Megfelelt			X	X	X	X	X	X	X	X	X	X	X	X
3.3.12.1.1.	*Az érintett szervezet:*	-		-		-			-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.1.1.2.	a naplózásra és elszámoltathatóságra vonatkozó eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a naplózási eljárásrendet.	Igen		Igen		Igen			N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.2.	Naplózható események	Megfelelt		Megfelelt		Megfelelt			X	X	X	X	X	X	X	X	X	X	X	X
3.3.12.2.1.	*Az érintett szervezet:*	-		-		-			-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.2.1.1.	meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.2.1.2.	egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;	Igen		Igen		Igen			N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.2.1.3.	megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.	Igen		Igen		Igen			N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.2.2.	Felülvizsgálat	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet meghatározott gyakorisággal felülvizsgálja és aktualizálja a naplózandó eseményeket.								N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.3.	Naplóbejegyzések tartalma	Megfelelt		Megfelelt		Megfelelt			X	X	X	X	X	X	X	X	X	X	X	X
3.3.12.3.1.	Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.3.2.	Kiegészítő információk	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer a naplóbejegyzésekben további, az érintett szervezet által meghatározott kiegészítő, részletesebb információkat is rögzít.								N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.3.3.	Központi kezelés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer biztosítja a meghatározott rendszerelemek által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását.								N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.4.	Napló tárkapacitás	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező		0	X	X	X	0	X	X	X	0	X	X	X
	Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.	Igen		Igen		Igen			N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.5.	Naplózást hiba kezelése	Megfelelt		Megfelelt		Megfelelt			0	X	X	X	0	X	X	X	0	X	X	X
3.3.12.5.1.	*Az elektronikus információs rendszer:*	-		-		-			-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.5.1.1.	naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.5.1.2.	elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.	Igen		Igen		Igen			N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.5.2.	Naplózási tárhely ellenőrzés	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét.								N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.5.3.	Valóideju riasztás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer riasztást küld, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik.								N	N	N	N	N	N	N	N	N	N	N	N

3.3.12.6.	Naplóvizsgálat és jelentéskészítés	Megfelelő		Megfelelő		Megfelelő		0	X	X	X	0	X	X	X	0	X	X	X
3.3.12.6.1.	*Az érintett szervezet:*	-	Kötelező	-	Kötelező	-	Kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.6.1.1.	rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából,	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.6.1.2.	jelenti ezeket a meghatározott személyeknek, vagy szerepköröknek.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.6.2.	Folyamatba illesztés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	X	X
	Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes, vagy tiltott tevékenységekre és történésekre reagál.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.6.3.	Összegzés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	X	X
	Az érintett szervezet megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes érintett szervezetre kiterjedő helyzetfelmérés érdekében.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.6.4.	Felügyeleti képességek integrálása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet egyesíti a naplóbejegyzések vizsgálatát a sebezhetőség ellenőrzési információkkal, a teljesítmény adatokkal, az elektronikus információs rendszer felügyeletéből származó információkkal, vagy egyéb forrásokból begyűjtött adatokkal vagy információkkal.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.6.5.	Összekapcsolás a fizikai hozzáférési információkkal	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet összefüggésbe hozza a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert információkkal.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.7.	Naplócsökkentés és jelentéskészítés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
3.3.12.7.1.	*Az elektronikus információs rendszer:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.7.1.1.	lehetőséget biztosít naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplóvizsgálati és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.7.1.2.	nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.7.2.	Automatikus feldolgozás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.8.	Időbélyegek	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.12.8.1.	*Az elektronikus információs rendszer:*	-	Kötelező	-	Kötelező	-	Kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.8.1.1.	belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.8.1.2.	időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.8.2.	Szinkronizálás	Nem kötelező		Nem kötelező		Megfelelő		0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.		Nem kötelező		Nem kötelező	Igen	Kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.9.	A naplóinformációk védelme	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.12.9.1.	Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.9.2.	Hozzáférés korlátozása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	0	X	0	0	X	X
	A naplófunkciók kezelésére csak az érintett szervezet által meghatározott, privilegizált felhasználók jogosultak.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N

3.3.12.9.3.	Fizikailag elkülönített mentés	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer a naplóbejegyzéseket meghatározott gyakorisággal elmenti, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.9.4.	Kriptográfiai védelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	0	X	0	0	0	0
	Kriptográfiai mechanizmusokat kell alkalmazni a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.10.	Letagadhatatlanság	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer védelmet biztosít az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.11.	A naplóbejegyzések megőrzése	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
	Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.12.	Naplógenerálás	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.12.12.1.	*Az elektronikus információs rendszer:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.12.12.1.1.	biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.12.2. pontban meghatározott, naplózható eseményekre;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.12.1.2.	lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.12.1.3.	naplóbejegyzéseket állít elő a 3.3.12.2. pont szerinti eseményekre a 3.3.12.3. pontban meghatározott tartalommal.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.12.12.2.	Rendszerszintű időalapú napló	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer a naplóbejegyzéseiből rendszerszintű (logikai vagy fizikai) felülvizsgálati naplót állít össze, amely - a felülvizsgálati napló egyedi bejegyzéseinek időbélyegei közötti kapcsolat tekintetében meghatározott tűréshatáron túli - időviszonyokat is tartalmazza.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.12.3.	Változtatások	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer biztosítja a lehetőséget a meghatározott személyeknek vagy szerepköröknek arra, hogy megváltoztassák az egyes rendszerelemekre végrehajtandó naplózást a kiválasztott esemény kritériumok alapján, meghatározott időtartamon belül.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N

3.3.	LOGIKAI VÉDELMI INTÉZKEDÉSEK							Követelmény											
		Bizalmasság		Sértetlenség		Rendelkezésre állás		B				S				R			
3.3.13.	RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	Megfelelt? (I/N)	Ki kell tölteni?	2	3	4	5	2	3	4	5	2	3	4	5
3.3.13.1.	Rendszer- és kommunikációvédelmi eljárásrend	Megfelelt		Megfelelt		Megfelelt		X	X	X	X	X	X	X	X	X	X	X	X
3.3.13.1.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.13.1.1.1.	megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.13.1.1.2.	a rendszer- és kommunikációvédelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.13.2.	Alkalmazás szétválasztás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	X	X	0	0	X	X
	Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.3.	Biztonsági funkciók elkülönítése	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.4.	Információmaradványok	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	X	X	0	0	0	0	0	0	0	0
	Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.5.	Túlterhelés - szolgáltatás megtagadás alapú támadás - állagi védelem	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Megfelelt	Kötelező	0	0	0	0	0	0	0	0	X	X	X	X
	Az elektronikus információs rendszer véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.					Igen		N	N	N	N	N	N	N	N	I	N	N	
3.3.13.6.	A határok védelme	Megfelelt	Kötelező	Megfelelt	Kötelező	Megfelelt	Kötelező	X	X	X	X	X	X	X	X	X	X	X	X
3.3.13.6.1.	*Az elektronikus információs rendszer:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.13.6.1.1.	felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.13.6.1.2.	a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.13.6.1.3.	csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.	Igen		Igen		Igen		N	I	N	N	N	I	N	N	N	I	N	N
3.3.13.6.2.	Hozzáférési pontok	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.3.	Külső kommunikációs szolgáltatások	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
3.3.13.6.3.1.	*Az érintett szervezet:*	-		-		-		-	-	-	-	-	-	-	-	-	-	-	-
3.3.13.6.3.1.1.	felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.3.1.2.	minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.3.1.3.	védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.3.1.4.	dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.3.1.5.	meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.4.	Alapeseti viszautasítás	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	Nem kötelező	0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat.							N	N	N	N	N	N	N	N	N	N	N	N

3.3.13.6.5.	Távoli készülékek megosztott csatornahasználatának tiltása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	X	X
	A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.6.	Hitelesített proxy kiszolgálók	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer hitelesített proxy - olyan szerver, számítógép vagy szerveralkalmazás, amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja - kiszolgálók segítségével irányítja a belső kommunikációs forgalmat a felügyelt interfészeken a meghatározott külső hálózatokhoz.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.7.	Biztonsági hibaállapot	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az elektronikus információs rendszer hibaállapotba kerül a határvédelmi eszköz működési hibája esetén.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.6.8.	Rendszerelemek elkülönítése	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet határvédelmi mechanizmusokat alkalmaz azoknak az elektronikus információs rendszerelemeknek az elkülönítésére, amelyek a meghatározott alapfeladatokat és alapfunkciókat támogatják.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.7.	Az adatátvitel bizalmassága	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	0	0	0	0	0	0
3.3.13.7.1.	Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.7.2.	Kriptográfiai vagy egyéb védelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	0	0	0	0	0	0
	Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.8.	Az adatátvitel sértetlensége	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	X	X	0	0	0	0
3.3.13.8.1.	Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.8.2.	Kriptográfiai vagy egyéb védelem	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	X	X	0	0	0	0
	Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.9.	A hálózati kapcsolat megszakítása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	0	0	0	0	X	X
	Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.10.	Kriptográfiai kulcs előállítása és kezelése	Megfelelő		Megfelelő		Megfelelő		X	X	X	X	X	X	X	X	X	X	X	X
3.3.13.10.1.	Az érintett szervezet előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.	Igen	Kötelező	Igen	Kötelező	Igen	Kötelező	N	I	N	N	N	I	N	N	N	I	N	N
3.3.13.10.2.	Rendelkezésre állás	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Az érintett szervezet előállítja, biztosítja az információk rendelkezésre állását abban az esetben is, amikor a kriptográfiai kulcsok elérhetetlenné válnak (elvesztés, sérülés, megsemmisülés).		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.11.	Kriptográfiai védelem	Megfelelő		Megfelelő		Nem kötelező		X	X	X	X	X	X	X	X	0	0	0	0
	Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.	Igen	Kötelező	Igen	Kötelező		Nem kötelező	N	I	N	N	N	I	N	N	N	N	N	N
3.3.13.12.	Együttműködésen alapuló számítástechnikai eszközök	Megfelelő		Nem kötelező		Nem kötelező		X	X	X	X	0	0	0	0	0	0	0	0
	Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.	Igen	Kötelező		Nem kötelező		Nem kötelező	N	I	N	N	N	N	N	N	N	N	N	N
3.3.13.13.	Nyilvános kulcsú infrastruktúra tanúsítványok	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	0	0
	Az érintett szervezet nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatótól.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.14.	Mobilkód korlátozása	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	0	0
3.3.13.14.1.	*Az érintett szervezet:*	-	Nem kötelező	-	Nem kötelező	-	Nem kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.13.14.1.1.	meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.14.1.2.	használati korlátozásokat vezet be, vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.14.1.3.	engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.15.	Elektronikus információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	0	0	0	0	0	0
3.3.13.15.1.	*Az érintett szervezet:*	-	Nem kötelező	-	Nem kötelező	-	Nem kötelező	-	-	-	-	-	-	-	-	-	-	-	-
3.3.13.15.1.1.	használati korlátozásokat vezet be, vagy megvalósítási útmutatót ad a VoIP technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat;							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.15.1.2.	engedélyezi, felügyeli és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.							N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.16.	Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)	Nem kötelező		Megfelelő		Nem kötelező		0	0	0	0	0	X	X	X	0	0	0	0

	Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.		Nem kötelező	Igen	Kötelező		Nem kötelező	N	N	N	N	N	I	N	N	N	N	N	N
3.3.13.17.	Biztonságos név/cím feloldó szolgáltatás (egyneveztett rekurzív vagy gyorsító tárat használó feloldás)	Nem kötelező		Megfelelő		Nem kötelező		0	0	0	0	0	X	X	X	0	0	0	0
	Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.		Nem kötelező	Igen	Kötelező		Nem kötelező	N	N	N	N	N	I	N	N	N	N	N	N
3.3.13.18.	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	Nem kötelező		Megfelelő		Nem kötelező		0	0	0	0	0	X	X	X	0	0	0	0
	Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.		Nem kötelező	Igen	Kötelező		Nem kötelező	N	N	N	N	N	I	N	N	N	N	N	N
3.3.13.19.	Munkaszakasz hitelessége	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	0	0	0	X	X	0	0	0	0
	Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.13.20.	Hibát követő ismert állapot	Nem kötelező		Nem kötelező		Nem kötelező		0	0	0	X	0	0	0	X	0	0	0	X
	Meghatározott hibatípusokhoz tartozó hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerül, amely a hiba esetén is megőrzi a rendszerállapot információkat.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.21.	A maradvány információ védelme	Nem kötelező		Nem kötelező		Nem kötelező		0	0	X	X	0	0	X	X	0	0	0	0
	Az elektronikus információs rendszer védi az érintett szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát; sértetlenségét.		Nem kötelező		Nem kötelező		Nem kötelező	N	N	N	N	N	N	N	N	N	N	N	N
3.3.12.22.	A folyamatok elkülönítése	Megfelelő		Megfelelő		Nem kötelező		X	X	X	X	X	X	X	X	0	0	0	0
	Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.	Igen	Kötelező	Igen	Kötelező		Nem kötelező	N	I	N	N	N	I	N	N	N	N	N	N