Az Ibtv.-ben meghatározott feladatok áttekintése a törvény hatálya alá tartozó szervezetek vonatkozásában

1. Bevezetés

Jelen dokumentum útmutató, amely segítséget kíván nyújtani a 2013 nyarán hatályba lépett **az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény** (a továbbiakban: **Ibtv.**) hatálya alá tartozó szervezeteknek. Az Ibtv. által előírt biztonsági osztályba és biztonsági szintbe sorolás követelményének határideje **2014. július 1.**

2. Jogszabályok

- **2013. évi L. törvény** - az állami és önkormányzati szervek elektronikus információbiztonságáról
- **301/2013. (VII.29.) Korm. rendelet** - a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról
- 484/2013. (XII. 17.) Korm. rendelet - a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
- **233/2013. (VI.30.) Korm. rendelet** - az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről
- **2012. évi CLXVI. törvény** - a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- **65/2013. (III.8.) Korm. rendelet** - a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
- **360/2013 (X.11.) Kormányrendelet –** az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- **541/2013. (XII. 30.) Korm. rendelet** - a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről
- **540/2013. (XII. 30.) Korm. rendelet** - a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről
- **26/2013. (X.21.) KIM rendelet** - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus

információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

- **73/2013. (XII.4.) NFM rendelet** - az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről
- **77/2013. (XII.19.) NFM rendelet** - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről
- **38/2011. (III.22.) Korm. rendelet** - a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról *(Módosulás várható)*
- **36/2013. (VII. 17.) BM rendelet** - a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról
- **16/2013. (VIII. 30.) HM rendelet** - a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről
- **34/2013. (VIII. 30.) NGM rendelet** - a Nemzeti Adó- és Vámhivatal elektronikusinformációs rendszerei biztonságának felügyeletéről és ellenőrzéséről.

3. Az Ibtv. hatálya alá tartozó szervezetek feladatai és kötelezettségei

3.1. Az Ibtv. hatálya alá tartozó szervezetek hatósági nyilvántartásba vételének szabályai

- A szervezetnek tevékenysége megkezdését megelőző 8 napon belül a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: Hatóság vagy NEIH) részére meg kell küldeni az informatikai biztonsági szabályzatot, valamint ha rendelkezésre áll, akkor a 2013. évi L. törvény 4.§-ában foglalt biztonsági tanúsítvány másolatát is - **73/2013. (XII.4.) NFM rendelet: 4.§**
- A szervezet az Ibtv. hatálya alá tartozó tevékenységének befejezését – ide értve a szervezet jogutódlással vagy jogutódlás nélkül történő megszűnését is – a tevékenység befejezésének időpontját megelőző 8 napon belül köteles bejelenteni a hatóság felé - **73/2013. (XII.4.) NFM rendelet: 5.§**
- A szervezet az Ibtv. hatálya alá tartozó tevékenysége megkezdését megelőző 8 napon belül a hatóság által az elektronikus tájékoztatás szabályai szerint közzétett elektronikus űrlap útján tesz eleget - **73/2013. (XII.4.) NFM rendelet: 2.§**
- A szervezet korábban megküldött adataiban történő változás esetén, a változást követő 8 napon belül kell megküldeni a hatóság részére - **73/2013. (XII.4.) NFM rendelet: 3.§ (3)**

- A szervezet vezetője köteles együttműködni a Hatósággal. Ennek során az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt, tájékoztatás céljából megküldi a szervezet informatikai biztonsági szabályzatát a Hatóság részére (előbbiek mellett az ellenőrzések lefolytatásához szükséges feltételeket is biztosítja). – Ibtv. 12.§ (3)

4. Az elektronikus információs rendszer biztonsági osztályba sorolása és a megfelelés felmérése

4.1.Az elektronikus információs rendszer biztonsági osztályba sorolása

- Az Ibtv. hatálya alá tartozó elektronikus információs rendszert biztonsági osztályba kell sorolni, bizalmasság, sértetlenség és rendelkezésre állás szempontjából, az **Ibtv. 7.§** -ában, valamint a **77/2013. (XII.19.) NFM rendelet 1.§ és 1. számú melléklet**ben rögzített követelményeknek megfelelően
- A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni – **Ibtv. 7.§ (3)**
- A szervezet vezetője az Ibtv.-ben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan – **Ibtv.7.§ (5)**
- A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni – **Ibtv. 8.§ (1)**
- Az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének eléréséhez a szervezetnek lehetősége van a biztonsági intézkedések fokozatos kivitelezésére – **Ibtv. 8. § (3)-(5)**.

4.2.Az elektronikus információs rendszer biztonsági osztálynak való megfelelés felmérése

- A szervezet a jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és ennek alapján meghatározza, hogy azok a vizsgálat elvégzésekor melyik biztonsági osztálynak felelnek meg – **Ibtv. 8. § (4)**
- A szervezet az elektronikus információs rendszerének aktuális állapotát a 77/2013. (XII. 19.) NFM rendelet 3. és 4. számú mellékletének figyelembe vételével összeveti a biztonsági osztályba sorolás eredményével.

5. A szervezet biztonsági szintbe sorolása és a megfelelés felmérése

5.1. A szervezet biztonsági szintbe sorolása

- Az Ibtv. hatálya alá tartozó szervezetet biztonsági szintbe kell sorolni. A biztonsági szintekbe sorolás a 77/2013. (XII.19.) NFM rendelet 2. melléklete alapján történik. Ezen felül meg kell állapítani a szervezet biztonsági szintjét, amely a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de legalább az **Ibtv. 9. § (2)** bekezdésében meghatározott biztonsági szintű – **Ibtv. 9.§**
- Ha a szervezet nem éri el a számára előírt biztonsági szintet, úgy az **Ibtv. 10. §**-a alapján lehetősége van a követelmények fokozatos teljesítésére – **Ibtv. 10. § (2)-(7)Ibtv. 10.§.**

5.2. A szervezet biztonsági szintnek való megfelelés felmérése

- A szervezet a jogszabályban meghatározott szempontok alapján meghatározza, hogy a vizsgálat elvégzésekor melyik biztonsági szintnek felel meg – **Ibtv. 10. § (1)**
- A szervezet biztonsági szintjének aktuális állapotát a **77/2013. (XII. 19.) NFM rendelet 3. és 4. számú mellékle**tének figyelembe vételével összeveti a biztonsági szintbe sorolás eredményével.

6. Cselekvési terv készítésének esetei

- Amennyiben a biztonsági osztályhoz kapcsolódó felmérés eredményeképpen a biztonsági osztályba sorolás eredményének nem felel meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet készít a szervezet a hiányosság megszüntetésére – **Ibtv**. **8. § (5)**
- Ha a vizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre a 2013. évi L. törvény 9. § (2) bekezdésében előírt biztonsági szint, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére érdekében **– Ibtv. 10.§ (2) és (7)**.

6.1. A cselekvési terv megvalósításának határideje

- az elektronikus információs rendszerre és szervezetre vonatkozó védelem elvárt erősségének eléréséhez a szervezetnek lehetősége van a biztonsági intézkedések fokozatos kivitelezésére. Ennek keretében az első vizsgálatkor megállapított biztonsági osztályt és szintet alapul véve, minden egyes következő, magasabb biztonsági osztályhoz és szinthez rendelt biztonsági intézkedések kivitelezésére két év áll rendelkezésére **–Ibtv. 8. § (3) és 10. § (4)**
- Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, akkor az 1. szint eléréséhez szükséges intézkedéseket a meghatározott szempontok szerint lefolytatott vizsgálatot követő egy éven belül meg kell valósítani – **Ibtv.10. § (3).**

7. Informatikai biztonsági incidensek bejelentése

- A szervezet érdekkörében felmerült vagy a tudomásra jutott biztonsági eseményeket be kell jelenteni a *Hatóság* részére - a közigazgatási hatósági eljárásról és szolgáltatásról szóló törvény szerint írásbelinek minősülő elektronikus úton. A minősített adatot tartalmazó bejelentést a szervezet papír alapon teszi meg - **73/2013. (XII.4.) NFM rendelet: 8.§.**
- Biztonsági eseménnyel kapcsolatban nem kizárólag a Nemzeti Elektronikus Információbiztonsági Hatóságnál lehet bejelentést tenni (elektronikus levélben, telefonon és faxon), hanem a *Kormányzati Eseménykezelő Központnál* (GovCERT) is **- Ibtv. 20. § (1) c) és 233/2013. (VI. 30.) Korm. rendelet 3. § (2) a)**
- Biztonsági eseménnyel kapcsolatban a kritikus infrastruktúrák tekintetében a *Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ* (LRLIBEK) is ellát incidenskezelési feladatokat **- 233/2013. (VI. 30.) Korm. Rendelet 8. § (3) a)**

8. A szervezet vezetőjének feladatai és kötelezettségei

8.1. A szervezet vezetője köteles együttműködni a Hatósággal. Ennek keretében

- Az Ibtv. 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt – **Ibtv. 12. § a)**
- A szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi, az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére – **Ibtv. 12.§ b) és c)** pontok
- A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről az **Ibtv. 11. §**-ában meghatározottak szerint
- Biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését – **Ibtv. 11.§ a)**
- Biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését – **Ibtv. 11.§ b)**
- Biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről – **Ibtv. 11.§ j)**
- Ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek – **Ibtv. 11.§ l)**
- Az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus

információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel – **Ibtv. 11.§ c)**

- Kiadja a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikáját – **Ibtv. 11.§ d)**
- Meghatározza a szervezet elektronikus információs rendszereinek informatikai biztonsági stratégiáját – **Ibtv.11.§ e)**
- Meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,– **Ibtv. 11.§ f).**
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról – **Ibtv. 11.§ g)**
- rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak – **Ibtv. 11.§ h)**
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek – **Ibtv. 11.§ k)**
- ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek – **Ibtv. 11.§ i)**
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért – **Ibtv. 11.§ m)**
- Az Ibtv. 11.§ (1) bekezdésben meghatározott feladatokért a szervezet vezetője a hivatkozott (1) bekezdés *k)* és *l)* pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni – **Ibtv. 11.§ (2)**
- A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén az Ibtv. 11.§ (1) és (2) bekezdésben írt feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató felett felügyeletet gyakorló miniszter biztosíttatja az érintett szolgáltatóval és a szervezet vezetőjével **–Ibtv. 11.§ (3)**

9. Az elektronikus információs rendszer biztonságáért felelős személy feladatai

9.1. Az elektronikus információs rendszer biztonságáért felelős személy feladatai az Ibtv. 13.§-a alapján

- Gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- Elvégzi vagy irányítja a fentiek szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- Előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- Előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- Kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal,
- Bármely elektronikus információs rendszerét érintő biztonsági eseményről történő tájékoztatás a 73/2013. (XII.4.) NFM rendeletben meghatározottak szerint tájékoztatni köteles az Ibtv.-ben meghatározott szervet,
- Amennyiben indokolt a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.
- Biztosítja az Ibtv-ben meghatározott követelmények teljesülését az Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő:
    a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők biztonsággal összefüggő tevékenysége esetén.
    b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők biztonsággal összefüggő tevékenysége esetén.
- Az Ibtv-ben meghatározott követelmények teljesüléséről jogosult a közreműködőtől tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.
- A helyszíni ellenőrzéssel érintett szervezet elektronikus információs rendszer biztonságáért felelős személye az Ibtv. **12. § c)** pontja alapján köteles a Hatósággal együttműködni.

10. Az elektronikus információs rendszer biztonságáért felelős személy alkalmazásának feltételei

- A **büntetlen előélet** követelményének való megfelelést a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni
- Nem kell a képzettséget megszereznie annak a személynek, aki rendelkezik a **26/2013. (X. 21.) KIM rendeletben** meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal – **26/2013. (X. 21.) KIM rendelet 7.§ (1) és (2) bekezdései**
- Az elektronikus információs rendszer biztonságáért felelős személy a közigazgatási és igazságügyi miniszter **26/2013. (X. 21.) KIM rendeletében** meghatározott rendszeres szakmai képzésen, továbbképzésen vesz részt.

Az elektronikus információs rendszer biztonságáért felelős személy az érintett szervezet igényeihez igazodva és annak rendelkezése szerint feladatát elláthatja:

a) részmunkaidőben,
b) a vonatkozó szerződésben meghatározott időtartamban, vagy
c) több érintett szervezetnél.

11. Fejlesztési projektekre vonatkozó előírások

- A központi, valamint az európai uniós forrásból megvalósuló fejlesztési projektek információbiztonsági követelményeinek teljesítése során a projekt vezetője a projekt tervezési szakában a hatóság részére véleményezésre megküldi a vonatkozó biztonsági osztályba sorolást és biztonsági szint meghatározást, továbbá mindazon dokumentációkat, amelyek alapján a biztonsági, és termékminősítési követelmények megvalósulása ellenőrizhető a projekt teljes életciklusára nézve, ideértve az átvétel, vagy teljesülés után az elektronikus információs rendszer használata során érvényesítendő elvárásokat is – **301/2013. Korm. rendelet 8.§ (1)**
- A projekt mérföldköveinek figyelembevételével, az adott projekt szakasz zárását megelőző legkevesebb harminc nappal kell a hatóság rendelkezésére bocsátani a kapcsolódó elektronikus információbiztonsági dokumentációt, hogy annak észrevételei, vagy kifogásai a projekt terveken, vagy a projekt tárgyán átvezethető és alkalmazható legyen – **301/2013. Korm. rendelet 8.§ (2)**
- A hatvan napnál rövidebb időtartamú projektek esetén az 301/2013. Korm. rendelet 8.§ (1) bekezdés szerinti dokumentációt legkésőbb a projekt befejezésekor kell a hatóság rendelkezésére bocsátani – **301/2013. Korm. rendelet 8.§ (3)**
- A Hatóság a 301/2013. Korm. rendelet 8.§ (1)–(3) bekezdés szerinti dokumentumok tekintetében a szakhatóság véleményét kikéri – **301/2013. Korm. rendelet 8.§ (4)**
- Az érintett szervezet – ha az elektronikus információs rendszer biztonságért felelős személy, szervezet kijelölése vagy az elektronikus informatikai biztonsági szabályzat elkészítése, az Ibtv.-ben meghatározott időn belül neki fel nem róható okból nem

teljesül – az Ibtv. 26. § (3) bekezdésében meghatározott hatvan, vagy kilencven napon belül a hatóságot tájékoztatja a teljesítést akadályozó ok és a teljesítés határidejének megjelölésével – **301/2013. Korm. rendelet 11.§**

12. Oktatással, képzettséggel kapcsolatos feladatok

A képzésről, a továbbképzésről és az éves továbbképzésről a **26/2013. (X.21.) KIM rendelet** rendelkezik. A miniszteri rendelet személyi hatálya **három** különböző szerepkörre terjed ki:

- **Elektronikus információs rendszer biztonságáért felelősszemély** (a szervezet vezetője által kinevezett személy, akit a NEIH felé is be kell jelenteni): az Ibtv. 13.§-ában foglalt feladatok ellátására kijelölt (megbízott) személy
- **Elektronikus információs rendszer védelméért felelős vezető**: az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat alapján, az Ibtv. hatálya alá tartozó egyéb szervek esetében munkaköri leírásban vagy egyéb módon kijelölt vezető
- **Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy**: állami és önkormányzati szervek esetében a szervezeti és működési szabályzat és a munkaköri leírások alapján, az Ibtv.hatálya alá tartozó egyéb szervek esetében a munkaköri leírásban vagy egyéb módon a feladatok ellátásával megbízott személy.

A rendelet megkülönböztet:

- **Képzést** (vizsgával zárul és az NKE bizonyítványt ad ki)
- **Továbbképzést** (vizsgával zárul és az NKE bizonyítványt ad ki), az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy és az elektronikus információs rendszerek védelméért felelős vezető.
- **Éves továbbképzést** (részvételről az NKE tanúsítványt állít ki), valamennyi szerepkört betöltő személy számára.

13. Mentesülések

13.1. Nem kell a képzésben részt venni az alábbi végzettségek esetén

- **CISA, CISM, CRISC vagy CISSP érvényes oklevéllel**
- vagy az alábbi **5 éves szakmai gyakorlat esetében**:
  a) az információbiztonsági irányítási rendszer
  aa) tervezése,
  ab) kialakítása,
  ac) működtetése során,
  b) az információbiztonsági ellenőrzés vagy felügyeleti tevékenység területén,
  c) az információbiztonsági kockázatelemzés területén,
  d) az elektronikus információs rendszerek információbiztonsági tanúsítási tevékenysége során, vagy
  e) az elektronikus információs rendszerek információbiztonsági tesztelésében (etikus hacker tevékenységben) szerzett szakmai tapasztalat.

A képzésbe történő felvétel előzetes felvételi követelménye a felsőfokú végzettség és legalább angol alapfokú komplex nyelvvizsga vagy ezzel egyenértékű bizonyítvány, oklevél.

13.2. Éves továbbképzés alól felmentés

Fontos, hogy az éves továbbképzés alól nincs felmentési lehetőség. Az egyes szerepkörökhöz kapcsolódó képzések adatai:

	Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy		
	Képzés	**Továbbképzés**	**Éves továbbképzés**
Időtartam/ maximális hiányzás	2 félév 300 óra / 10 %	50 óra/év /10 %	25 óra/év /10 %
Tárgykör	a) információbiztonsági szervezési ismeretek,	a) információbiztonsági technológiai ismeretek,	a) információbiztonsági technológiai ismeretek,
	b) kockázatértékelés és menedzsment,	b) informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek,	b) informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek,
	c) stratégia és szervezeti támogatás,	c) kockázatértékelés és biztonsági események kezelése (incidenskezelés),	c) jogi és szervezetirányítási ismeretek.
	d) biztonsági események	d) jogi és	

	Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy		
	Képzés	**Továbbképzés**	**Éves továbbképzés**
	kezelése (incidenskezelés),	közigazgatási ismeretek.	
	e) jogi, vezetéselméleti és technológiai ismeretek az információbiztonságban.		
Gyakoriság	Egyszer	Egyszer	Évente egyszer

	Elektronikus információs rendszer védelméért felelős vezető		
	Képzés	**Továbbképzés**	**Éves továbbképzés**
Időtartam/ maximális hiányzás	2 félév 300 óra / 10 %	8 óra/év / 10%	8 óra/év / 10%
Tárgykör	a) információbiztonsági szervezési ismeretek,	a) jogi, közigazgatási, vezetéselméleti és szervezeti ismeretek,	a) jogi, közigazgatási, vezetéselméleti és szervezetirányítási ismeretek,
	b) kockázatértékelés és menedzsment,	b) információbiztonsági technológiai ismeretek,	b) információbiztonsági technológiai ismeretek,
	c) stratégia és szervezeti támogatás,	c) informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek	c) informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek.
	d) biztonsági események kezelése (incidenskezelés),		
	e) jogi, vezetéselméleti és technológiai ismeretek az információbiztonságban.		
Gyakoriság	Egyszer	Egyszer	Évente egyszer

	Elektronikus információs rendszer biztonságáért felelős vezető		
	Képzés	**Továbbképzés**	**Éves továbbképzés**
Időtartam/ maximális hiányzás	2 félév 300 óra / 10 %	-	50 óra/év /10 %
Tárgykör	a) információbiztonsági szervezési ismeretek,		a) információbiztonsági technológiai ismeretek,
	b) kockázatértékelés és menedzsment,		b) kockázatértékelés és biztonsági események kezelése (incidenskezelés),
	c) stratégia és szervezeti támogatás,		c) informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek,
	d) biztonsági események kezelése (incidenskezelés),		d) jogi és szervezetirányítási ismeretek.
	e) jogi, vezetéselméleti és technológiai ismeretek az információbiztonságban.		a) információbiztonsági technológiai ismeretek,
Gyakoriság	Egyszer	-	Évente egyszer