

Az IBSZ hatálya feltétlenül kiterjed-e minden munkavállalóra, vagy lehet szelektíven értelmezni, pl. a fizikai dolgozók kivétele?

VFP2 KiberVéd - NIS2 Audit felkészítés szakértői
állásfoglalás 2026/36

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.24	Kálmán és Társa Ügyvédsdi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A Kiberbiztonsági törvény¹ az információbiztonsági szabályzatot (a gyakorlatban: IBSZ) nem a munkavállalók, hanem a felhasználók és az elektronikus információbiztonsági követelmények szabályozásának eszközeként határozza meg. A végrehajtási rendelet² pedig azt várja el, hogy a szabályzat maga jelölje ki a saját hatókörét, a képzési, hozzáférési és személyi biztonsági követelményeket pedig következetesen az elektronikus információs rendszerek felhasználóihoz, illetve a hozzáférés megadásához köti. Ebből az következik, hogy a jogszabály nem kívánja meg, hogy az IBSZ személyi hatálya automatikusan és teljes terjedelmében kiterjedjen minden munkavállalóra. A szűkítés tehát megengedett, sőt bizonyos mértékig kifejezetten elvárt.

A szűkítés helyes mércéje azonban nem a munkakör jellege (fizikai vagy szellemi), hanem a tényleges hozzáférés. Az a munkavállaló, aki a munkája során semmilyen módon nem használja a szervezet elektronikus információs rendszereit, és nem fér hozzá az azokban kezelt adatokhoz, kiberbiztonsági értelemben nem felhasználó, ezért rá a felhasználói kötelezettségek és a biztonságtudatossági képzés nem irányadó. Aki viszont akár minimális hozzáféréssel rendelkezik (ideértve a termelésirányítási, raktári vagy kiber-fizikai rendszereket is), az felhasználó, számára azonban elegendő a szerepköréhez igazított, szűkített szabályzati kivonat és képzés.

Két korlátot hangsúlyozunk. Egyrészt a szervezetnek minden munkakört kockázati szempontból be kell sorolnia, így a kivétel nem lehet hallgatólágos, hanem dokumentált döntés eredménye. Másrészt a teljes IBSZ válogatás nélküli terjesztése nemcsak felesleges, hanem a rendelet szerint kifejezetten kerülendő, mert a szabályzat jogosulatlanok általi megismerése önmagában biztonsági kockázat.

2. PROBLÉMAFELVETÉS

A NIS2-felkészülés során visszatérő gyakorlati kérdés, hogy az IBSZ-t és a hozzá kapcsolódó biztonságtudatossági képzést a szervezet teljes létszáma ki kell-e terjeszteni. A kérdés különösen a jelentős fizikai állománnyal működő szervezeteknél (gyártás, logisztika, közüzemek, egészségügyi kiegészítő személyzet) éles, ahol a dolgozók egy része soha nem jelentkezik be semmilyen rendszerbe. A teljes körű kiterjesztés mellett szól a látszólagos biztonság („mindenki aláírta”), ellene szól a költség, a szervezési teher és az a tapasztalat, hogy a nem releváns szabályok tömeges kihirdetése rontja a szabályzat hitelességét.

Az auditori gyakorlatban a kérdés két irányból is felmerül. Egyfelől hiányosságként értékelhető, ha a szabályzat személyi hatálya „minden munkavállaló”, de a képzési nyilvántartás csak az irodai állományt fedi le: ilyenkor a szervezet a saját szabályzatát nem tartja be. Másfelől hiányosság az is, ha a szabályzat hallgat a hatályról, és a fizikai dolgozók kihagyása csak szóbeli

¹ Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági törvény). A hivatkozott szöveg a 2026. július 29. napjától hatályos állapot.

² A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: Rendelet). A 2. melléklet követelményeinél az „A”, „J”, „M” jelölés az „alap”, a „jelentős”, illetve a „magas” biztonsági osztályban kötelező követelményt, az „O” az egyik osztályban sem kötelező (opcionális) követelményt jelöli.

gyakorlat, dokumentált kockázati döntés nélkül. A jó válasz tehát nem a „mindenkire” vagy a „senkire”, hanem a pontosan meghatározott és megindokolt hatókör.

A vizsgált szakértői vélemény lényege, hogy a hatály szűkítése megengedett, a szűkítés alapja a hozzáférés hiánya, a részleges hozzáféréssel rendelkezőknek szerepalapú kivonat és képzés jár, a teljes IBSZ minden munkavállalóra történő ráerőltetése pedig információszivárgási kockázatot hordoz. Az alábbiakban ezt az álláspontot vetjük össze a hatályos jogszabályi szöveggel, és ahol szükséges, árnyaljuk.

3. VÁLASZ

Az IBSZ hatálya szelektíven, a felhasználói körre szűkítve is meghatározható, és ez a jogszabályi szöveghez közelebb álló megoldás, mint a teljes állományra kiterjesztett hatály.

Aki fizikai értelemben sem ér az EIR-hez, és nem fér hozzá védendő adathoz, az nem felhasználó, ezért a NIS2-követelmények felhasználói oldala rá nem vonatkozik. Az állítás azonban csak a funkcionális teszttel együtt igaz. A „fizikai dolgozó” munkajogi vagy bérszámfejtési kategória, nem kiberbiztonsági fogalom. Egy gépkezelő, aki érintőpanelen paraméterez, egy targoncás, aki raktárirányítási terminált használ, vagy egy műszakvezető, aki a termelésirányítási rendszerben nyugtáz, a törvény EIR-fogalma alapján felhasználó, függetlenül a munkakörének besorolásától. A kivétel alapja ezért soha nem a munkakör címkéje, hanem a 14.2.1. pont szerinti besorolás és a fiókkezelési nyilvántartás³ egybevetése.

A hatályt a szabályzatban kifejezetten és logikusan rögzíteni kell, és ehhez a Rendelet 1.1.1.2. pontja kötelező alapot ad. A „felhasználói jogosultsággal rendelkező munkavállalók” fordulat helyett azonban tágabb megfogalmazást javasunk, mert a felhasználói kör túlnyúlik a munkavállalókon (szerződéses partnerek, kölcsönzött munkavállalók, gyakornokok, külső üzemeltetők), és mert egyes rendelkezések (fizikai belépés, incidensek észlelése és jelentése) a nem felhasználókat is érinthetnek.

A kiberbiztonsági szabályozás a képzést nem a munkaviszonyhoz, hanem a rendszerhasználathoz köti, ezért a hozzáféréssel nem rendelkezők valóban kihagyhatók. A minimális hozzáféréssel rendelkező műszakvezető esetében a jogszabályi minimum három elemből áll: a hozzáférés megadása előtt a rá vonatkozó hozzáférési szabályok megismerése és dokumentált elfogadása⁴, a szerepköréhez igazított képzés⁵, valamint mindezek nyilvántartása⁶. Egy néhány oldalas felhasználói kivonat és egy rövid, célzott oktatás ezt teljes egészében kielégíti.

A teljes IBSZ minden munkavállalónak történő kiosztása két hibát egyszerre valósít meg: a nem felhasználókat olyan kötelezettségekkel terheli, amelyeket nem tudnak értelmezni, a rendszerek belső működéséről szóló ismereteket pedig a szükségesnél szélesebb körben teszi hozzáférhetővé.

³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.2.4.1. pont (a rendszerben engedélyezett felhasználók meghatározása); A, J, M.

⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.9.3.1. pont; A, J, M.

⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 3.9.1.1. pont; A, J, M.

⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 3.13.1. pont; A, J, M.

A szűkített hatály nem jelenti azt, hogy a nem felhasználók a kiberbiztonsági rendszeren teljesen kívül maradnak. A fizikai belépésre jogosultak listája⁷, az ad hoc belépők kísérése⁸ és a szabályszegés fegyelmi következménye⁹ a szervezet bármely tagját érintheti, ha az EIR-nek helyet adó helyiségekbe belép, vagy biztonsági eseményt észlel. Ezért a hatály szűkítése mellett néhány, mindenkre vonatkozó alapszabályt (idegenek jelzése, talált adathordozó kezelése, belépőkártya átadásának tilalma) célszerű a belépéskori tájékoztatóban vagy az általános munkáltatói szabályzatban elhelyezni, az IBSZ-től függetlenül.

4. GYAKORLATI JAVASLATOK

- a) *Hatály klauzula alkalmazása az IBSZ-ben.* Javasolt megfogalmazás: „A szabályzat személyi hatálya kiterjed mindazon természetes személyekre, akik a Szervezet elektronikus információs rendszereit használják, azokhoz vagy az azokban kezelt adatokhoz hozzáféréssel rendelkeznek, illetve ilyen hozzáférést igényelnek, függetlenül a jogviszonyuk jellegétől (munkavállaló, vezető tisztségviselő, kölcsönzött munkavállaló, szerződéses partner munkatársa). A felhasználói kör meghatározása a munkaköri kockázati besorolás és a felhasználói fiókok nyilvántartása alapján történik.”
- b) *Dokumentumszerkezet tekintetében az IBSZ törzsdokumentuma* tartalmazza a hatókört, a szerepköröket, a felelőségeket és az elveket; a technikai eljárásrendek (naplózás, konfiguráció, mentés, incidenskezelés) külön, korlátozott hozzáférésű mellékletekben szerepeljenek. A felhasználóknak egy rövid 5-20 oldalas felhasználói információbiztonsági kézikönyv készül, amelyet a hozzáférés megadása előtt megismernek és aláírnak.
- c) A 14.2.1. pont szerinti *munkakörök kockázati besorolását* a HR munkaköri jegyzékére építve érdemes elkészíteni, „nincs EIR-hozzáférés” kategóriával. Ez a lista az audit során a kivétel bizonyítéka; felülvizsgálatát a munkakörök változásához¹⁰ kell kötni.
- d) A 3.13.1. pont szerinti *képzési nyilvántartásban* a felhasználói lista és a képzésen részt vettek listája legyen egymással összevethető. Az eltérés mindkét irányban auditmegállapítás alapja lehet: képzetlen felhasználó éppúgy, mint a szabályzatban vállalt, de el nem végzett teljes körű képzés.
- e) A hatály szűkítéséről szóló döntést az *IBSZ vezetői jóváhagyása*¹¹ fedi le. Az elektronikus információs rendszer biztonságáért felelős személy a szabályzat előkészítése és véleményezése során ellenőrzi, hogy a hatály, a munkaköri besorolás és a képzési terv egymással összhangban áll.

⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.2.1. pont; A, J, M.

⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.6.4. pont; A, J, M.

⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.12.1. pont; A, J, M.

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.8.1. pont; A, J, M.

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.1.1.4. pont; A, J, M.

5. A JOGSZABÁLYI KERET

5.1 Kinek szól az IBSZ a törvény szerint?

A Kiberbiztonsági törvény a szervezet vezetőjének feladatai között az IBSZ címzettjeit is megnevezi. A vezető

7. kiadja a felhasználókra és az elektronikus információbiztonsági követelményekre vonatkozó információbiztonsági szabályzatot, valamint gondoskodik annak legalább két évente vagy a jogszabályban meghatározott esetekben történő felülvizsgálatáról; [2024. évi LXIX. törvény 6. § (3) bekezdés 7. pont]

A törvény szövege tehát a „felhasználókra” vonatkozó szabályzatról beszél, nem a munkavállalókra vagy a szervezet teljes személyi állományára vonatkozóan. A Rendelet ezt azzal egészíti ki, hogy a hatókör meghatározását magára a szabályzatra bízza. Már az „alap” biztonsági osztályban is kötelező követelmény, hogy az IBSZ

1.1.1.2. meghatározza a célkitűzéseket, a ható- és szerepköröket, a felelőségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.1.1.2. pont; A, J, M]

A hatókör meghatározása így nem lehetőség, hanem kötelező tartalmi elem. A szervezet e körben mérlegelési joggal rendelkezik, a mérlegelés eredményét azonban rögzítenie kell, és annak összhangban kell állnia a kockázatelemzéssel.

Munkajogi oldalról az IBSZ a munkáltató egyoldalú belső szabályzata. A munka törvénykönyve szerint

(1) A munkáltató a 15–16. §-ban meghatározott jognyilatkozatait általa egyoldalúan megállapított belső szabályzatban vagy egyoldalúan kialakított gyakorlat érvényesítésével (a továbbiakban együtt: munkáltatói szabályzat) is megteheti. [2012. évi I. törvény 17. § (1) bekezdés]

A munkáltatói szabályzat személyi hatályát a munkáltató maga állapítja meg; a munkajog nem követeli meg, hogy minden belső szabályzat minden munkavállalóra vonatkozzon. Azt viszont igen, hogy a szabályzat a címzettjei számára megismerhető legyen, ami a szerepkör szerinti kivonatok gyakorlatát is alátámasztja.

5.2 A képzési kötelezettség személyi köre

A törvény szerint a szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében

a) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a szervezet munkatársainak – az informatikáért felelős miniszter rendeletében meghatározott – kiberbiztonsági képzéséről, továbbképzéséről; [2024. évi LXIX. törvény 6. § (5) bekezdés a) pont]

A „szervezet munkatársai” fordulat első olvasatra a teljes állományra utalhat. A rendelkezés azonban a részleteket miniszteri rendeletre utalja, és a képzési rendelet¹² normaszövege kizárólag a vezető és az elektronikus információs rendszer biztonságáért felelős személy képzését szabályozza. A rendelet indokolása kifejezetten rögzíti, hogy a munkatársak szervezeten belüli képzésére vonatkozó elvárásokat a 7/2024. (VI. 24.) MK rendelet már tartalmazza, ezért azokat a képzési rendelet nem ismétli meg.¹³ A munkatársi képzés személyi körét tehát a Rendelet 2. melléklete határozza meg, amely a címzetteket nem a munkaviszonyhoz, hanem a rendszerhasználathoz köti:

3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is): 3.2.1.1. Az új felhasználók kezdeti képzése keretében, majd ezt követően a szervezet által meghatározott gyakorisággal. [7/2024. (VI. 24.) MK rendelet 2. melléklet 3.2.1. pont; A, J, M]

A szerepkör alapú képzés címzettje ugyancsak a felhasználó, a kötelezettség pedig a hozzáférés engedélyezéséhez kapcsolódik:

3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak: 3.9.1.1. Az EIR-hez vagy az információhoz való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően, továbbá azt követően a szervezet által meghatározott rendszerességgel. [7/2024. (VI. 24.) MK rendelet 2. melléklet 3.9.1. pont; A, J, M]

A képzési kötelezettség személyi köre tehát a jogszabály rendszertani értelmezése alapján a felhasználók köre. Ez a kör egyfelől szűkebb a munkavállalók körénél (a rendszereket nem használó dolgozók kimaradnak), másfelől tágabb annál, mert a vezetőket és a rendszerhez hozzáférő szerződéses partnereket, kölcsönzött munkavállalókat is magában foglalja. A NIS2 irányelv ugyanezt a logikát követi: a vezető testületek tagjainak képzését kötelezővé teszi, a munkavállalók rendszeres képzését a tagállamok által ösztönzendő elvárásként fogalmazza meg, a kockázatkezelési intézkedések között pedig az alapvető kiberhigiéniai gyakorlatokat és a kiberbiztonsági képzést nevesíti.¹⁴

5.3 A hozzáférés a kulcstényező

A hozzáférési szabályok megismertetése és elfogadtatása a hozzáférést igénylő személyekhez kötődik. A szervezet

¹² A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet 12. § (2) bekezdés c) és g) pont. E rendelkezések a Kiberbiztonsági törvény 1. § (1) bekezdés a)–c) és f) pontja, valamint 1. § (2a) bekezdése szerinti szervezetekre, továbbá a kritikus és az ország védelme és biztonsága szempontjából jelentős szervezetekre alkalmazandók [418/2024. (XII. 23.) Korm. rendelet 1. § (2) bekezdés].

¹³ A Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről szóló 17/2025. (VII. 24.) EM rendelet 3. § (1) bekezdés (az elektronikus információs rendszer biztonságáért felelős személy: évente legalább 20 óra továbbképzés) és 4. § (1) bekezdés (a szervezet vezetője: egy éven belül legalább 8 órás képzés, majd évente legalább 4 órás továbbképzés).

¹⁴ A 17/2025. (VII. 24.) EM rendelet indokolása, Nemzeti Jogszabálytár: <https://njt.jog.gov.hu/jogszabaly/2025-17-K3-8Y>. Az indoklás nem normaszöveg, a jogalkotói szándék értelmezéséhez azonban irányadó.

14.9.3. Ellenőrzi, hogy a szervezeti információkhoz és rendszerekhez hozzáférést igénylő személyek 14.9.3.1. a hozzáférés megadása előtt megismerték és dokumentált módon elfogadták a vonatkozó hozzáférési szabályokat; [7/2024. (VI. 24.) MK rendelet 2. melléklet 14.9.3. pont; A, J, M]

Van azonban egy követelmény, amely valóban minden munkakörre kiterjed, és amely a kivétel dokumentált alapját adja. A szervezet

14.2.1. minden szervezeti munkakörhöz hozzárendel egy kockázati besorolást; [7/2024. (VI. 24.) MK rendelet 2. melléklet 14.2.1. pont; A, J, M]

A szervezetnek a fizikai munkaköröket is be kell sorolnia, és éppen ez a besorolás igazolja, hogy az adott munkakör nem jár EIR-hozzáféréssel. A fizikai dolgozók kihagyása tehát nem a szabályzat hallgatásán, hanem a munkaköri kockázati besoroláson alapul, amely egyúttal az audit során bemutatható bizonyíték. Ugyanebbe az irányba mutat, hogy a biztonsági szerepköröket és felelőségeket a munkaköri leírásokba is be kell építeni¹⁵: a hozzáférés nélküli munkakör leírása ezt a tényt is rögzítheti.

5.4 A szabályzat védelme és a szerepkör szerinti megismertetés

A teljes IBSZ válogatás nélküli kihirdetése ellen a Rendelet két helyen is állást foglal. Az IBSZ-re vonatkozó alapkövetelmény szerint a szervezet

1.1.3. Gondoskodik arról, hogy az információbiztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.1.3. pont; A, J, M]

A szabályzat tehát maga is védendő információ. A naplózási beállítások, a hálózati szegmentálás, a mentési rend vagy az incidenskezelés technikai részletei olyan ismeretek, amelyek a bizalmasság törvényi fogalma szerint csak az arra jogosultak számára és csak a jogosultságuk szintjéig ismerhetők meg. Ezek tömeges terjesztése a szervezet saját támadási felületét növeli.

A Rendelet emellett valamennyi szabályzati követelménycsoportnál (hozzáférés-felügyelet, tudatosság és képzés, naplózás, személyi biztonság) azonos fordulattal írja elő, hogy a szervezet a szabályzatot és az eljárásrendet

Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint [7/2024. (VI. 24.) MK rendelet 2. melléklet 3.1.1. pont; A, J, M]

A jogalkotó tehát nem „mindenkivel”, hanem a „szervezet által meghatározott személyekkel szerepkörük szerint” való megismertetést vár el. A szerepalapú kivonatok készítése így nem könnyítés, hanem a rendelet szövegének megfelelő megoldás. A „jelentős” és a „magas” osztályban ezt a legkisebb jogosultság elve is megerősíti:

2.60. A szervezet a legkisebb jogosultság elvét alkalmazza, és a felhasználók vagy a felhasználók nevében eljáró folyamatok számára csak a számukra kijelölt feladatok

¹⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.13. pont; A, J, M.

végrehajtásához szükséges hozzáféréseket engedélyezi. [7/2024. (VI. 24.) MK rendelet 2. melléklet 2.60. pont; J, M]

6. A DOKUMENTUMBAN ELŐFORDULÓ RELEVÁNS FOGALMAK

Elektronikus információs rendszer (EIR): a Kiberbiztonsági törvény fogalma tágabb a hétköznapi „informatikai rendszer” kifejezésnél, mert kifejezetten magában foglalja a kiber-fizikai rendszereket is:

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy [2024. évi LXIX. törvény 4. § 24. pont b) alpont]

Ennek a kérdés szempontjából különös jelentősége van: egy gyártósori vezérlő, egy raktári vonalkódolvasó vagy egy gépkezelői érintőpanel ugyanúgy EIR lehet, mint az irodai munkaállomás.

Információbiztonsági szabályzat (IBSZ): a törvény az „információbiztonsági szabályzat” kifejezést használja; a gyakorlatban elterjedt „informatikai biztonsági szabályzat” elnevezés és az IBSZ rövidítés ugyanezt a dokumentumot jelöli. A szabályzat kiadása és legalább kétévenkénti felülvizsgálata a szervezet vezetőjének feladata.

Felhasználó: sem a Kiberbiztonsági törvény, sem a Rendelet nem határozza meg. A törvény értelmező rendelkezései csak a „felhasználó szervezet” és a „regisztrált felhasználói jogosultság” fogalmát ismerik. A jogszabályi szöveggörnyezet (a képzési, hozzáférési és fiókkezelési követelmények) alapján felhasználó az a természetes személy, aki a szervezet EIR-jét használja, vagy az abban kezelt adatokhoz hozzáfér, függetlenül attól, hogy munkavállaló, vezető vagy szerződéses partner. Ez a funkcionális megközelítés összhangban áll a törvény alapelvével, amely szerint a védelmet az adatkezelésre használt eszközök, az eljárások, valamint

c) az a) és b) pontban foglaltakat kezelő személyek [2024. évi LXIX. törvény 5. § (2) bekezdés c) pont]

együttetésére nézve kell biztosítani.

Bizalmasság: a törvény fogalma a kérdés egyik ágának, a szabályzat terjesztési körének megítéléséhez ad támpontot:

az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról; [2024. évi LXIX. törvény 4. § 13. pont]

7. FORRÁSOK

1. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

2. 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
3. 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
4. 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
5. 17/2025. (VII. 24.) EM rendelet a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről, valamint a rendelet indokolása (Nemzeti Jogszabálytár)
6. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv)
7. 2012. évi I. törvény a munka törvénykönyvéről