

A NIS2-kompatibilis információbiztonsági szabályozás és egyéb dokumentumok jóváhagyása és kihirdetése

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/34

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.02	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A kiberbiztonsági jogszabályok a szabályozási dokumentumoknál nem aláírást, hanem jóváhagyást, kiadást vagy döntést írnak elő. Aláírást a jogalkotó csak kivételesen és kifejezett szöveggel kíván meg. A jóváhagyás azonban jognyilatkozat, amelynek megtörténtét, időpontját és a jóváhagyó személyét a szervezetnek az auditon és a hatóság előtt bizonyítania kell, ezért dokumentált formára mindenképpen szükség van.

A jóváhagyó személye dokumentumtípusonként eltér. Az alábbi döntéseket a jogszabály a szervezet vezetőjének tartja fenn:

- az információbiztonsági szabályzat (IBSZ) kiadását,
- a biztonsági osztályba sorolást

- az elektronikus információs rendszer (EIR) használatbavételéről vagy továbbhasználatáról szóló döntést, ez utóbbit a rendelet kifejezetten át nem ruházhatónak minősíti.

A rendszerbiztonsági tervet a vezető vagy az elektronikus információs rendszer biztonságáért felelős személy (IBF) hagyhatja jóvá, a biztonságértékelési tervet az engedélyezésért felelős személy vagy kijelölt képviselője, az eltéréseket a vezető vagy a kockázatok felvállalására jogosult személy. A stratégiák, eljárásrendek és nyilvántartások jóváhagyóját a jogszabály nem nevezi meg, ezt a szervezet az IBSZ-ben határozza meg.

A jóváhagyás jogi formáját a kiberbiztonsági jogszabályok nem írják elő, ezért az általános szabályok irányadók. Teljes bizonyító erejű magánokirat egyik dokumentumnál sem követelmény. Az írásbeliség a Ptk. és az Mt. szerint elektronikus formában is teljesül, ha a tartalom változatlanul visszaidézhető, a nyilatkozó személye és a nyilatkozat időpontja pedig azonosítható. Ezt egy hitelesített felhasználóhoz kötött, naplózott és az IBSZ-ben szabályozott jóváhagyási munkafolyamat (például M365 vagy Google Workspace környezetben) is teljesítheti. A vezetőnek fenntartott döntéseknél és a hatóságnak megküldött dokumentumoknál ugyanakkor a saját kezű vagy a minősített elektronikus aláírást javasoljuk.

A kihirdetés jogszerű módja a szerepkör szerinti kiadás és megismertetés. A közös mappa és a körlevél a közzététel elfogadható eszköze, önmagában azonban nem bizonyítja a megismerést, a teljes IBSZ válogatás nélküli terjesztése pedig a rendeletbe ütközhet. Az auditon a jóváhagyott hatályos verzió, a kiadás időpontja, a címzetti kör, valamint a nyilatkozatok, képzési nyilvántartások és rendszernaplók együttese bizonyítja a kihirdetést.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban: Szervezet) elkészítette a kiberbiztonsági szabályozását: az IBSZ-t, a rendszerbiztonsági terveket, a folyamatos felügyeleti stratégiát, a biztonságértékelési tervet, a biztonsági osztályba sorolást, valamint a kapcsolódó eljárásrendeket és nyilvántartásokat. Két kérdés merült fel.

1. Dokumentumok aláírása

Kötelező-e az egyes dokumentumtípusokat aláírni, és ha igen, kinek, a szervezet vezetőjének, vagy a feladat átvadható az informatikai vezetőnek vagy az IBF-nek? Vannak-e alá nem írandó dokumentumok? Milyen jogi formában kell aláírni: teljes bizonyító erejű magánokiratként, egyszerű aláírással, szervezeti elektronikus aláírással vagy bélyegzővel? Elegendő-e, ha a belső rendszer (például M365 vagy Google Workspace) jogosultságkezelése tanúsítja a jóváhagyást?

2 Kihirdetés

Elegendő-e a közös mappába helyezés és egy körlevél a kollégáknak, és hogyan bizonyítható a kihirdetés az auditon?

A dokumentumok tartalmi követelményei és a hatósági bejelentések részletszabályai nem tárgyai ennek az állásfoglalásnak.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2 irányelv)

3. VÁLASZ

3.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik, felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el, és két évente kiberbiztonsági auditra kötelezett.² A válasz lényege a többi szervezettípusra is irányadó, az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek többletkötelezettségeit a 3.6. pont foglalja össze.

A Kiberbiztonsági tv. a szervezet vezetőjének fogalmát nem határozza meg. Gazdasági társaságnál ez a törvényes képviselő, azaz a vezető tisztségviselő (ügyvezető, vezérigazgató vagy az igazgatóság).³

3.2 A jogszabályok jóváhagyást várnak el, nem aláírást

A Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet a dokumentumoknál következetesen a „kiadja”, „jóváhagyja”, „dönt” és „dokumentumban rögzíti” fordulatokat használja. Az aláírás a szervezet saját dokumentumainál csak kivételesen jelenik meg. A 418/2024. (XII. 23.) Korm. rendelet a sérülékenységvizsgálati alapidokumentum kötelező tartalmi elemeként írja elő

*14. a szervezet vezetőjének vagy az általa meghatalmazott, a szervezet vezetőjének szervezetszerű helyettesítésére jogosult vezető aláírását.
[418/2024. (XII. 23.) Korm. rendelet 53. § (2) bekezdés 14. pont]*

A védelmi intézkedések között két, egyik biztonsági osztályban sem kötelező követelmény kívánja meg, hogy a munkavállalók aláírásukkal ismerjék el a munkaviszony megszűnése után is fennálló kötelezettségeiket.⁴ Ahol tehát a jogalkotó aláírást akart, azt kimondta. Az aláírás ezért a szabályozási dokumentumoknak nem érvényességi kelléke: egy alá nem írt, de a vezető által igazolhatóan jóváhagyott és kiadott IBSZ létező és hatályos szabályzat.

A jóváhagyás ugyanakkor jognyilatkozat, amelynek meglétét az auditor és a hatóság vizsgálja. A rendelet a használatbavételi döntésnél a „jegyzőkönyvben dokumentált módon” fordulattal, a törvény a besorolás „dokumentált módon” történő felülvizsgálatával⁵ egyértelművé teszi, hogy a döntésnek utólag ellenőrizhető nyomot kell hagynia, az auditor pedig jogosult minden, a biztonsággal kapcsolatba hozható dokumentum megismerésére.⁶ A kérdés tehát nem az, hogy kell-e aláírni, hanem az, hogy a jóváhagyás ténye, ideje és a jóváhagyó személye hogyan bizonyítható; az aláírás ennek legkevésbé vitatható, de nem egyetlen eszköze.

3.3 Ki hagyja jóvá az egyes dokumentumokat?

3.3.1 A vezetőnek fenntartott döntések

Az IBSZ kiadása a szervezet vezetőjének törvényi feladata. A vezető

² 2024. évi LXIX. tv. 16. § (1) bekezdés és 23. § (1) bekezdés b) pont

³ 2013. évi V. tv. 3:29. § (1) bekezdés

⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.6.2. és 14.10.2. pont (O)

⁵ 2024. évi LXIX. tv. 10. § (7) bekezdés

⁶ 1/2025. (I. 31.) SZTFH rendelet 5. § (3) bekezdés

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. tv. 6. § (3) bekezdés 7. pont]

A rendelet ezt személyes felelősséggel egészíti ki. Az IBSZ

1.1.1.4. A szervezet vezetője által kerül jóváhagyásra, aki felelősséget vállal és elszámoltatható a szervezeti műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a szervezeti eszközök, személyek, más szervezetek szempontjából számottevőnek tartott kockázatokért. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.1.1.4. pont] (A, J, M)

Az IBSZ egyúttal munkáltatói szabályzat.⁷ A munkajog a munkáltatói jogkör gyakorlásának rendjét a munkáltatóra bízta⁸, a kiberbiztonsági szabályozás azonban szűkebb: a kiadást és a jóváhagyást név szerint a szervezet vezetőjéhez telepíti, és a vezető mulasztását külön bírsággal fenyegeti.⁹ Álláspontunk szerint ezért az IBSZ jóváhagyása az informatikai vezetőre vagy az IBF-re nem ruházható át. Az IBF szerepe az előkészítés és a véleményezés; a közsférában ezt a rendelet kifejezetten így írja elő¹⁰, a többi szervezetnél pedig abból következik, hogy az IBF-nek minden védelmet érintő döntés előkészítésében részt kell vennie.¹¹ Aki előkészít, az nem hagyhatja jóvá a saját munkáját. Jóváhagyóként az járhat el, aki a létesítő okirat vagy a szervezeti és működési szabályzat szerint a vezető jogkörét gyakorolja, akadályoztatás esetén a szervezetszerű helyettes.

A biztonsági osztályba sorolás a második vezetői döntés:

(2) A biztonsági osztályba sorolásról a szervezet vezetője dönt, és felel annak a jogszabályoknak és kockázatoknak való megfeleléséért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolás eredményét a szervezet az elektronikus információs rendszerek nyilvántartásában vagy egyéb belső szabályzatban rögzíti. [2024. évi LXIX. tv. 10. § (2) bekezdés]

A rendelet szerint a besorolást a szervezet vezetője hagyja jóvá¹², a szervezetnek pedig ellenőriznie kell, hogy a vezető a besorolási döntést jóváhagyta.¹³ A döntés nem delegálható, az előkészítés viszont az IBF feladata.¹⁴ A jóváhagyás tárgya nem feltétlenül önálló irat: a vezető által jóváhagyott nyilvántartási verzió vagy egy besorolási határozat egyaránt megfelel.

⁷ 2012. évi I. tv. 17. § (1) bekezdés

⁸ 2012. évi I. tv. 20. § (1) és (2) bekezdés

⁹ 2024. évi LXIX. tv. 30. § (3) bekezdés; a rendelkezés a nemzeti kiberbiztonsági hatóságot nevesíti

¹⁰ 418/2024. (XII. 23.) Korm. rendelet 12. § (2) bekezdés c) és g) pont

¹¹ 2024. évi LXIX. tv. 11. § (6) bekezdés a) pont

¹² 7/2024. (VI. 24.) MK rendelet 1. melléklet 2.1.2. pont

¹³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.2.3. pont (A, J, M)

¹⁴ 418/2024. (XII. 23.) Korm. rendelet 12. § (2) bekezdés d) pont

A harmadik döntés a rendszer használatbavétele vagy továbbhasználata:

1.1.6. a szervezet a rendszer biztonsági állapotára vonatkozó dokumentumok (rendszerbiztonsági terv, értékelési jelentés, rendszer kockázatelemzés, intézkedési terv) alapján az üzembe helyezésére vagy üzemben tartására vonatkozó kockázatokat megvizsgálja, és a szervezet vezetője más személyre át nem ruházható feladatkörében eljárva – jegyzőkönyvben dokumentált módon – dönt a rendszer használatbavételéről vagy használatának folytatásáról; [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.6. pont]

Ez az egyetlen dokumentum, amelynél a jogszabály a formát (jegyzőkönyv) és az átruházás tilalmát is kimondja; a jegyzőkönyvben célszerű a döntés alapjául szolgáló dokumentumok verzióját is megjelölni.

3.3.2 Megosztható jóváhagyások

A rendszerbiztonsági tervnél a rendelet választást enged:

A szervezet a biztonsági követelményeket a rendszerbiztonsági tervben dokumentálja, amelyet a szervezet vezetője vagy az elektronikus információs rendszer biztonságáért felelős szerepkört betöltő személy hagy jóvá. [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.3. pont]

A védelmi intézkedések között a terveket „a jóváhagyó felelős” tekinti át és hagyja jóvá a végrehajtás előtt.¹⁵ A terv jóváhagyása tehát az IBF-re bízható, ha ezt az IBSZ így rendeli. Egy korlát van: a terv a biztonsági osztályt is dokumentálja¹⁶, a besorolásról azonban a vezető dönt, így az IBF által jóváhagyott terv csak a vezető által már jóváhagyott besorolást veheti át.

A biztonságértékelési tervnél a rendelet az engedélyezési szerepkörhöz igazodik. A szervezet

5.2.3. Biztosítja, hogy a biztonságértékelési tervet az engedélyezésre jogosult felelős vagy kijelölt képviselője az értékelés elvégzése előtt felülvizsgálja és jóváhagyja. [7/2024. (VI. 24.) MK rendelet 2. melléklet 5.2.3. pont] (A, J, M)

Az engedélyezésért felelős személyt a szervezet jelöli ki az adott EIR-hez¹⁷, így a tervet ez a személy vagy kijelölt képviselője hagyja jóvá. Az értékelést végző és a jóváhagyó ne legyen azonos, mert az értékelés függetlenségét külön követelmények védik.¹⁸

A védelmi intézkedésektől való eltéréseket és a helyettesítő intézkedéseket a szervezet vezetője vagy a kockázatok felvállalására jogosult szerepkört betöltő személy hagyja jóvá.¹⁹ Ha az IBSZ

¹⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2.1.14. pont (A, J, M)

¹⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2.1.6. és 15.2.2. pont (A, J, M)

¹⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 5.12.1. pont (A, J, M)

¹⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 5.3. pont (J, M) és 5.4. pont (A, J, M)

¹⁹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.1.3. és 4.2.4. pont

a kockázati vezetőt vagy a kockázatkezelésért felelős személyt²⁰ ilyen jogkörrel ruházta fel, a jóváhagyás átadható; ennek hiányában a vezetőé marad.

3.3.3 Dokumentumok megnevezett jóváhagyó nélkül

A kockázatmenedzsment stratégiát és a folyamatos felügyeleti stratégiát a szervezet határozza meg és rögzíti dokumentumban²¹, jóváhagyót a rendelet nem nevez meg. Mivel a kockázatmenedzsment keretrendszert a törvény szerint a vezető hozza létre és működteti²², és a keretrendszer a szervezet kockázattűrő képességét is rögzíti²³, a szervezeti szintű stratégiák vezetői jóváhagyását javasoljuk. A rendszerszintű folyamatos felügyeleti stratégia²⁴ jóváhagyása az IBF-re bízható.

A szakterületi szabályzatokat és eljárásrendeket (hozzáférés-felügyelet, naplózás, incidenskezelés és a többi követelménycsoport) a rendelet azonos szerkezetű követelménnyel kezeli. A szervezet

2.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint

[...]

2.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.1.1. és 2.1.2. pont] (A, J, M)

A kiadás felelősét tehát a szervezet jelöli ki. Az IBSZ rendelkezhet úgy, hogy a szakterületi szabályzatokat a vezető, az eljárásrendeket az informatikai vezető vagy az IBF adja ki, feltéve, hogy az IBSZ a kiadmányozási rendet rögzíti, és az alsóbb szintű dokumentum az IBSZ-szel nem ellentétes.

A nyilvántartások, jelentések és tervek (az EIR-nyilvántartás, a kockázatelemzés, az értékelési jelentés, az intézkedési terv, a képzési nyilvántartás²⁵) nem jóváhagyandó szabályozók, hanem a működés bizonyítékai. Ezeket nem kell aláírni; hitelességüket a keltezés, a verziószám, a felelős megjelölése és az őket kezelő rendszer adja.

A felhasználói oldalon a hozzáférés engedélyezése előtt a felhasználó dokumentált nyilatkozatban igazolja, hogy a rá vonatkozó biztonsági és hozzáférési szabályokat megismerte és elfogadta.²⁶ A rendelet itt sem aláírást, hanem dokumentált nyilatkozatot kíván, ezért az elektronikus elfogadás megfelel.

A megállapításokat az alábbi táblázat foglalja össze.

²⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.20. pont (A, J, M)

²¹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.1.1.2. és 1.1.1.1.3. pont, valamint 2. melléklet 1.10. és 1.23. pont (A, J, M)

²² 2024. évi LXIX. tv. 6. § (2) bekezdés

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.19.1.4. pont (A, J, M)

²⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 5.15. pont (A, J, M)

²⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.5., 15.4., 5.2.5., 5.10. és 3.13.1. pont (A, J, M)

²⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3.2. és 14.9.3.1. pont (A, J, M)

Dokumentum	Jóváhagyó a jogszabály szerint	Átruházható-e	Javasolt forma
Információbiztonsági szabályzat	szervezet vezetője	nem (előkészítő: IBF)	vezetői aláírás
Biztonsági osztályba sorolás	szervezet vezetője	nem (előkészítő: IBF)	jóváhagyott nyilvántartás vagy határozat, vezetői aláírással
Használatbavételi, továbbhasználati döntés	szervezet vezetője	kifejezetten nem	jegyzőkönyv, vezetői aláírással
Rendszerbiztonsági terv	vezető vagy IBF	igen, az IBF-re	dokumentált jóváhagyás
Biztonságértékelési terv	engedélyezésért felelős vagy kijelölt képviselője	igen	dokumentált jóváhagyás
Eltérések, helyettesítő intézkedések	vezető vagy kockázatok felvállalására jogosult	igen, ha az IBSZ kijelöli	dokumentált jóváhagyás, indokolással
Kockázatmenedzsment és folyamatos felügyeleti stratégia	nincs megnevezve	igen	vezetői jóváhagyás javasolt
Szakterületi szabályzatok, eljárásrendek	a szervezet által kijelölt személy	igen	az IBSZ kiadmányozási rendje szerint
Nyilvántartások, kockázatelemzés, jelentések, intézkedési terv	nincs jóváhagyó	nem értelmezhető	keltezett, verziózott bizonyíték, aláírás nélkül
Felhasználói nyilatkozatok	a felhasználó	nem	dokumentált (akár elektronikus) nyilatkozat

3.4 A jóváhagyás jogi formája

3.4.1 Írásbeliség és bizonyító erő

Mivel a kiberbiztonsági jogszabályok a jóváhagyás formájáról hallgatnak, az általános polgári jogi és munkajogi szabályok irányadók. A Ptk. szerint

(2) Ha e törvény eltérően nem rendelkezik, a jognyilatkozat akkor minősül írásba foglaltnak, ha jognyilatkozatát a nyilatkozó fél aláírta.
(3) Írásba foglaltnak kell tekinteni a jognyilatkozatot akkor is, ha annak közlésére a jognyilatkozatban foglalt tartalom változatlan visszaidézésére, a nyilatkozattevő személyének és a nyilatkozat megtétele időpontjának azonosítására alkalmas formában kerül sor. [2013. évi V. tv. 6:7. § (2) és (3) bekezdés]

Az IBSZ-re mint munkáltatói szabályzatra az Mt. hasonló szabálya vonatkozik: írásbelinek kell tekinteni a jognyilatkozatot, ha közlése a benne foglalt információ változatlan visszaidézésére, a nyilatkozattevő személyének és a nyilatkozat időpontjának azonosítására alkalmas elektronikus

dokumentumban történik.²⁷ Az írásbeliséget tehát nem csak a saját kezű aláírás teljesíti. A Kúria tanácsadó testületének többségi álláspontja szerint az e-mail vagy más elektronikus közlés is írásbeli, ha a három feltétel a konkrét esetben fennáll; hamisíthatatlanság nem szükséges.²⁸

A teljes bizonyító erejű magánokirat más kategória: nem az érvényesség, hanem a bizonyítás szabálya. Ilyen erővel bír többek között az az okirat, amelyet a jogi személy képviselőjére jogosult személy a rá vonatkozó szabályok szerint megfelelően aláírt²⁹, továbbá az elektronikus okirat, ha

f) az elektronikus okiraton az aláíró a minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy bélyegzőjét helyezte el, [...] [2016. évi CXXX. tv. 325. § (1) bekezdés f) pont]

Teljes bizonyító erőt a kiberbiztonsági jogszabályok egyetlen dokumentumnál sem kívánnak meg. A kiberbiztonsági audit nem per: az auditor dokumentumvizsgálattal, interjúval és teszttel győződik meg a megfelelésről³⁰, és a jóváhagyás hitelt érdemlő igazolását várja el. A teljes bizonyító erő hatósági eljárásban, munkaügyi vagy kártérítési vitában és a vezetői felelősség vizsgálatakor válik fontossá, ami a vezetőnek fenntartott döntéseknél az erősebb forma mellett szól.

3.4.2 Papír, elektronikus aláírás, bélyegző

A saját kezű, cégszerű aláírás papíron a hagyományos megoldás, teljes bizonyító erővel. A minősített elektronikus aláírás az uniós jog szerint a saját kezű aláírással azonos joghatású³¹, és a minősített tanúsítványon alapuló fokozott biztonságú aláírással együtt teljes bizonyító erejű magánokiratot hoz létre. Az egyszerű vagy nem minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás (a legtöbb kereskedelmi aláíró platform alapszolgáltatása) az írásbeliséget a Ptk. 6:7. § (3) bekezdése szerint teljesítheti, teljes bizonyító erővel azonban nem rendelkezik; belső dokumentumokhoz ez is megfelelő.

A szervezeti elektronikus bélyegző a jogi személyhez, nem természetes személyhez kötődik. Igazolja, hogy a dokumentum a szervezettől származik és nem módosult, arról azonban nem tanúskodik, hogy a vezető a tartalmat személyesen jóváhagyta. A bélyegző ezért a kiadmányozásra és a hatóságnak történő megküldésre alkalmas, a vezetői jóváhagyás nyomát mellette a munkafolyamatban vagy egy aláírt kiadási lapon kell megőrizni.

3.4.3 Elegendő-e a jogosultságkezelés által rögzített jóváhagyás?

A kérdés lényege, hogy pótolja-e az aláírást, ha a dokumentumkezelő rendszer (M365, Google Workspace vagy más rendszer) naplója tanúsítja, hogy a vezető a dokumentumot jóváhagyta. Álláspontunk szerint igen, meghatározott feltételekkel. A Ptk. 6:7. § (3) bekezdése és az Mt. 22. § (2) bekezdése nem aláírást, hanem három tulajdonságot kíván: a tartalom változatlan

²⁷ 2012. évi I. tv. 22. § (2) bekezdés a) pont

²⁸ A Kúria Új Ptk. Tanácsadó Testületének véleménye a jognyilatkozat írásbeliségének követelményeiről a Ptk. 6:7. § (3) bekezdésének alkalmazásában (kuria-birosag.hu).

²⁹ 2016. évi CXXX. tv. 325. § (1) bekezdés d) pont

³⁰ 1/2025. (I. 31.) SZTFH rendelet 2. § (2) bekezdés

³¹ Az Európai Parlament és a Tanács 910/2014/EU rendelete (eIDAS) 25. cikk (2) bekezdés

visszaidézhetőségét, a nyilatkozó személyének és a nyilatkozat időpontjának azonosíthatóságát. Egy jóváhagyási munkafolyamat ezt teljesíti, ha

- a jóváhagyó személyét többtényezős hitelesítéssel védett, kizárólag általa használt felhasználói fiók azonosítja;
- a jóváhagyás kifejezett cselekmény (jóváhagyó gomb, munkafolyamat-lépés), nem pusztán a fájl megnyitása vagy szerkesztése;
- a jóváhagyott verzió utóbb nem módosítható, a módosítás új verziót és új jóváhagyást igényel;
- a napló időbélyeggel rögzíti a jóváhagyást, a rendszergazda sem tudja észrevétlenül átírni, a megőrzési idő legalább két auditciklust lefed, és a bejegyzés rendszertől függetlenül bemutatható formában exportálható;
- az IBSZ vagy a dokumentumkezelési szabályzat ezt a munkafolyamatot a jóváhagyás elfogadott módjaként rögzíti, mert a jognyilatkozatok alaki rendjét a munkáltató határozza meg.³²

A megoldás gyengesége a bizonyító erő és a rendszerfüggőség, a napló nem teljes bizonyító erejű magánokirat, hitelességét vita esetén szakértővel kell alátámasztani, a szolgáltatóváltás vagy a naplóbeállítások módosítása pedig a bizonyítékot elveszítheti. Ezért kétszintű rendet javasunk, a vezetőnek fenntartott három döntést és a hatóságnak megküldött dokumentumokat saját kezű vagy minősített elektronikus aláírással kell ellátni, a többi dokumentumnál a szabályozott munkafolyamat elegendő. Ha a szervezet az IBSZ-t is munkafolyamatban hagyja jóvá, a vezető által aláírt egyoldalas kiadási lap (a dokumentum megnevezése, verziószáma, a jóváhagyás és a hatálybalépés napja) pótolja a hiányzó aláírást.

3.5 A dokumentumok kihirdetése

3.5.1 Kiadás, kihirdetés, megismertetés

A rendelet három lépcsőt különböztet meg. Az IBSZ-t a szervezet „kidolgozza és kihirdeti”³³, a szakterületi szabályzatokat „kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint”. A rendszerbiztonsági tervet a meghatározott személyek és szerepkörök megismerik³⁴, a viselkedési szabályokat a szervezet „a szervezeten belül kihirdeti”³⁵, a kockázatelemzés eredményeit pedig a meghatározott személyekkel megismerteti.³⁶ A kiadás a hatályos szöveg formális rögzítése, a kihirdetés a közzététel, a megismertetés pedig annak biztosítása, hogy a címzettek a rájuk vonatkozó szabályokat ténylegesen ismerjék; a három lépcső egymást nem pótolja.

A munkajog a kihirdetés mércéjét is megadja:

(2) A munkáltatói szabályzatot közzétenek kell tekinteni, ha azt a helyben szokásos és általában ismert módon közzéteszik. [2012. évi I. tv. 17. § (2) bekezdés]

³² 2012. évi I. tv. 20. § (2) bekezdés és 22. § (1) bekezdés

³³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.1.1. pont (A, J, M)

³⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2.2. pont (A, J, M)

³⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3.1. pont (A, J, M)

³⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.4.5. pont (A, J, M)

Az írásbeli jognyilatkozat közzétételnek tekinthető, ha az elektronikus dokumentum a címzett számára hozzáférhetővé válik.³⁷ A közzététel helyét és módját tehát a szervezet választja meg, ha az a munkatársak számára ismert és a dokumentum ténylegesen elérhető.

A kihirdetésnek korlátja is van. 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)

Ugyanez vonatkozik a rendszerbiztonsági tervre.³⁸ A kihirdetés ezért nem jelenthet válogatás nélküli terjesztést: a technikai mellékleteket (naplózás, hálózati architektúra, mentési rend) a szerepkör szerinti címzettek kapják, a felhasználók a rájuk vonatkozó kivonatot és a viselkedési szabályokat.

3.5.2 A közös mappa és a körlevél

A közös mappába helyezés és a körlevél a közzététel elfogadható módja, ha az IBSZ ezt a helyet hivatalos közzétételi csatornaként megnevezi, a mappa csak olvasható és a címzetti körre korlátozott, a hatályos verzió egyértelműen azonosítható, a korábbi verziók pedig archívumba kerülnek. A körlevél a dokumentumot, a verziószámot, a hatálybalépés napját, az érintettek körét és az elérési helyet nevezi meg. A teljes IBSZ e-mail mellékletként történő továbbítása nem alkalmas erre, mert a szöveg ellenőrizetlenül továbbítható, ami az 1.1.3. ponttal ellentétes.

A körlevél a megismertetést nem bizonyítja, a kézbesítés igazolható, az elolvasás nem. A megismerést a dokumentált nyilatkozat, az olvasási visszaigazolást rögzítő intranetes vagy e-learning megoldás, valamint a képzés és annak nyilvántartása bizonyítja.³⁹ A nyilatkozat elektronikus úton is megtehető, ha a személy és az időpont azonosítható. A szabályok módosításakor a nyilatkozatot meg kell ismételni.⁴⁰

3.5.3 A kihirdetés bizonyítása az auditon

Az auditor a védelmi intézkedések vizsgálatának módszereként dokumentumvizsgálatot, interjút és tesztet alkalmaz.⁴¹ A kihirdetést ezért a munkatársak tudásával is vizsgálhatja, megkérdezheti, hol találják a hatályos szabályzatot, és ellenőrizheti, hogy a közzétételi hely elérhető-e. Az auditra a következő bizonyítékokat célszerű előkészíteni:

- a) a jóváhagyott, keltezett és verziószámmal ellátott hatályos dokumentumot a jóváhagyás bizonyítékával (aláírás, kiadási lap vagy munkafolyamat-napló) és a verziótörténettel;
- b) a kiadás és a kihirdetés időpontját és módját (a közzététel helye, a körlevél vagy intranetes hír, a dokumentumkezelő rendszer naplója), valamint a szerepkörök és dokumentumok összerendelését;
- c) a megismerés bizonyítékát, azaz a felhasználói nyilatkozatokat, az olvasási visszaigazolásokat, a képzési jelenléti íveket vagy e-learning naplókat, összevetve az aktuális felhasználói listával;

³⁷ 2012. évi I. tv. 24. § (1) bekezdés

³⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2.5. pont (A, J, M)

³⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3.2., 14.9.3.1., 3.2.1. és 3.13.1. pont (A, J, M)

⁴⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3.4. és 14.9.3.2. pont (A, J, M)

⁴¹ 1/2025. (I. 31.) SZTFH rendelet 2. § (2) bekezdés a)-c) pont

- d) a közzétételi hely jogosultsági beállításait, amelyek igazolják, hogy a teljes IBSZ-t és a rendszerbiztonsági tervet csak az arra jogosultak érik el;
- e) a korábbi verziók archívumát, amelyből megállapítható, hogy egy adott időpontban melyik szöveg volt hatályos.

A cél az, hogy a jóváhagyás, a kiadás, a kihirdetés és a megismertetés láncolata dokumentumokkal megszakítás nélkül követhető legyen.

3.6 A közzétételhez tartozó szervezetek közzétételiségei

Ha a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) vagy f) pontja alá tartozik, az IBSZ-t a hatály alá kerülést követő 180 napon belül meg kell küldenie a nemzeti kiberbiztonsági hatóságnak⁴², amely azt nyilvántartásba veszi.⁴³ A megküldés az IBF feladata a vezető jóváhagyását követően⁴⁴, elektronikus úton, a hatóság által meghatározott formátumban, a bejelentett adatokat igazoló dokumentumokkal együtt.⁴⁵ A nyilvántartásba vételi kérelem elmulasztása bírsággal jár.⁴⁶ A benyújtott IBSZ-nek ezért olyan formában kell léteznie, amely a vezetői jóváhagyást a szervezeten kívül is igazolja: ez a vezető minősített elektronikus aláírása vagy a szervezet minősített bélyegzője a jóváhagyott verzió.

Ugyanezeknél a szervezeteknél a használatbavételről vagy továbbhasználatról hozott vezetői döntést a hatóság hagyja jóvá.⁴⁷ Az IBSZ-t soron kívül felül kell vizsgálni, ha a rendszer biztonságát érintő változás következik be, új kockázat merül fel, vagy az ellenőrzés és az audit hiányosságot tár fel.⁴⁸ Minden módosítás új jóváhagyást, kiadást és kihirdetést igényel, a módosított IBSZ-t pedig ismét meg kell küldeni a hatóságnak.

3.7 A javasolt eljárás

A jóváhagyási és kihirdetési rendet az IBSZ-ben célszerű rögzíteni:

- a) Kiadmányozási rend, az IBSZ-ben rögzíteni, hogy melyik dokumentumtípust ki hagyja jóvá és ki adja ki, mely döntések nem ruházhatók át, és ki a vezető helyettese.
- b) Aláírási forma, a vezetőnek fenntartott döntéseknél és a hatóságnak megküldött dokumentumoknál saját kezű vagy minősített elektronikus aláírás, a többi dokumentumnál szabályozott jóváhagyási munkafolyamat.
- c) Munkafolyamat, többszörös hitelesítés, kifejezett jóváhagyó lépés, verziózárolás, időbélyeges és exportálható napló, legalább két auditciklusnyi megőrzés.
- d) Formai elemek, minden szabályozó dokumentumon verziószám, a jóváhagyó neve és beosztása, a jóváhagyás és a hatálybalépés napja, a címzetti kör.
- e) Kihirdetés, egy kijelölt, csak olvasható és jogosultsághoz kötött közzétételi hely verziótörténettel; a körlevél a közzététel tényét, helyét és a hatálybalépést közli, a teljes IBSZ-t nem tartalmazza.

⁴² 2024. évi LXIX. tv. 8. § (4) bekezdés e) pont

⁴³ 2024. évi LXIX. tv. 28. § (1) bekezdés 1. pont l) alpont

⁴⁴ 418/2024. (XII. 23.) Korm. rendelet 12. § (2) bekezdés c) pont

⁴⁵ 418/2024. (XII. 23.) Korm. rendelet 8. § (1) bekezdés

⁴⁶ 418/2024. (XII. 23.) Korm. rendelet 2. melléklet 4. sor

⁴⁷ 418/2024. (XII. 23.) Korm. rendelet 14. § (1) és (2) bekezdés

⁴⁸ 418/2024. (XII. 23.) Korm. rendelet 6. §

- f) Megismertetés, szerepkör szerinti kivonatok és képzés, nyilatkozat a hozzáférés megadása előtt és minden módosítás után, a nyilatkozatok összevetése a felhasználói listával.
- g) Bizonyítékcsoomag, dokumentumtípusonként összeállítva: jóváhagyás, kiadás, kihirdetés, megismerés, hozzáférés-korlátozás és verzióarchívum.
- h) Hatósági benyújtás az a)-c) és f) pont szerinti szervezeteknél a jóváhagyott IBSZ és minden módosítása minősített aláírással vagy bélyegzővel, a hatóság formátumában.

4. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (eIDAS), az (EU) 2024/1183 rendelettel módosított szöveg
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.)
- 2016. évi CXXX. törvény a polgári perrendtartásról (Pp.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- A Kúria Új Ptk. Tanácsadó Testületének véleménye a jognyilatkozat írásbeliségének követelményeiről a Ptk. 6:7. § (3) bekezdésének alkalmazásában