HIVATALOS ÉRTESÍTŐ

22. szám

A MAGYAR KÖZLÖNY MELLÉKLETE

2025. április 30., szerda

Tartalomjegyzék

I. Utasítások

III. Közlemények

I. Utasítások

A honvédelmi miniszter 9/2025. (IV. 30.) HM utasítása a kijelölt vezetői kör részére történő kiberbiztonsági incidenskezeléssel összefüggő azonnali beszámolás rendjéről

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontja alapján a következő utasítást adom ki:

1. Általános rendelkezések

1. § Az utasítás hatálya a honvédelmi szervezetekre terjed ki.

2. § A Honvédelmi Minisztérium (a továbbiakban: HM) Portfóliókezelő Főosztály főosztályvezetője tájékoztatja az utasításban foglaltakról az egyes állami tulajdonban álló gazdasági társaságok felett az államot megillető tulajdonosi jogok és kötelezettségek összességét gyakorló személyek kijelöléséről szóló 1/2022. (V. 26.) GFM rendelet 1. melléklet VII. táblázatában foglalt, a HM tulajdonosi joggyakorlása alá tartozó gazdasági társaságok vezetőit.

3. § Az utasítást a honvédelmi ágazati elektronikus információbiztonsági eseménykezelés rendjéről szóló 3/2023. (II. 24.) HM utasítás 22. § (1) bekezdés c) és d) pontjában meghatározott esetekre kell alkalmazni.

4. § Az utasítás alkalmazásában

a) *beszámolás:* a 8. § szerinti kijelölt vezetői kör részére a kiberbiztonsági incidenssel összefüggésben zárt katonai információs rendszer, illetve telekommunikációs szolgáltatás útján végzett jelentés vagy riasztás és értesítés,

b) *értesítés:* a kiberbiztonsági incidenskezelés során az utasításban foglaltak alapján a riasztás kiadásáról szóló, visszaigazolást nem igénylő jelzés,

c) *jelentés:* a kiberbiztonsági incidenskezelés során az utasításban foglalt magas kategóriába sorolt kiberbiztonsági incidensközeli helyzettel összefüggő, előre meghatározott elemeket tartalmazó megosztott információ,

d) *kiberbiztonsági incidens:* a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 4. § 46. pontjában meghatározott fogalom,

e) *kiberbiztonsági incidenskezelés:* a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 4. § 47. pontjában meghatározott folyamat,

f) *kiberbiztonsági incidensközeli helyzet:* a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 4. § 49. pontjában meghatározott fogalom,

g) *kijelölt vezetői kör:* a 8. § szerinti és az általuk kijelölt politikai és katonai vezető beosztású személyek,

h) *riasztás:* a kiberbiztonsági incidenskezelés során az utasításban foglalt kritikus kategóriába sorolt kiberbiztonsági incidensekkel összefüggő, kötelező elemeket tartalmazó intézkedést vagy reagálást igénylő megosztott információ.

2. Az azonnali beszámolás speciális részletszabályai

5. § (1) Az ágazati kiberbiztonsági incidenskezeléssel összefüggésben végzett beszámolás során a kiberbiztonsági incidens első szintű kategorizálása érdekében az incidenskezelő a saját hatáskörben végzett döntéséhez az alábbi elveket veszi figyelembe:

a) magas besorolású kategóriába esnek azok a kiberbiztonsági incidensközeli helyzetek, amelyek a bejelentés időpontjában számosságukban és hatásukban súlyosan befolyásoló tényezőként vagy fenyegetettségként jelennek meg az érintett rendszer vagy a rendszer felhasználói vonatkozásában,

b) kritikus besorolású kategóriába esnek a kiberbiztonsági incidensek, amelyek a bejelentés időpontjában számosságukban és hatásukban igazoltan korlátozó tényezőként vagy fenyegetettségként jelennek meg az érintett rendszer vagy a rendszer felhasználói vonatkozásában.

(2) A magas besorolású kiberbiztonsági incidensközeli helyzetek esetén a kijelölt vezetői kör részére jelentést kell küldeni.

(3) A kritikus besorolású kiberbiztonsági incidensek esetén a kijelölt vezetői kört riasztani és értesíteni kell.

6. § (1) A honvédelmi kiberbiztonsági incidenskezelő központ végzi az ágazati kiberbiztonsági incidenskezeléssel összefüggő bejelentések fogadását, illetve azokról a kijelölt vezetői kör részére történő beszámolást.

(2) Az (1) bekezdésben meghatározott beszámolás nem érinti a Magyar Honvédség (a továbbiakban: MH) Kibertér Ügyeletes Parancsnok (a továbbiakban: KIÜP) saját hatáskörben történő tájékoztatási tevékenységét.

7. § (1) A KIÜP végzi az MH rendszereit érintő és az MH üzemeltetési és kiberbiztonsági incidenskezelési körébe tartozó, a kiberbiztonsági incidensben érintett szervezetek vonatkozásában a Honvéd Vezérkar (a továbbiakban: HVK) főnöke (a továbbiakban: HVKF) és a HVKF útján a honvédelmi miniszter tájékoztatását is. Ezzel egy időben a KIÜP végrehajtja a Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) kibertér műveleti szakfeladatokra kijelölt szervezeti egységének értesítését.

(2) A honvédelmi kiberbiztonsági incidenskezelő központ végzi az ágazati kiberbiztonsági incidensekről – az MH rendszerei kivételével – a HM katonai nemzetbiztonság irányításáért felelős államtitkár (a továbbiakban: HM KNIFÁT) és a HM KNIFÁT útján a honvédelmi miniszter tájékoztatását.

8. § (1) A kijelölt vezetői körbe a kijelölés a zárt katonai információs rendszerben létrehozott, a jelentési terv alapján szervezett csoportokba történő felvétellel történik, amelynek karbantartását

a) a HM azonnali jelentési csoportra vonatkozóan a honvédelmi minisztertől kapott feladatszabás,

b) a KNBSZ azonnali jelentési csoportra vonatkozóan a KNBSZ főigazgatójától kapott feladatszabás és

c) a HVK azonnali jelentési csoportra vonatkozóan a HVKF rendelkezése alapján a KIÜP-től kapott feladatszabás

alapján a honvédelmi kiberbiztonsági incidenskezelő központ hajtja végre.

(2) A HVK azonnali jelentési csoportba további személyek felvételére a KNBSZ főigazgatója tehet javaslatot a HVKF részére.

(3) A jelentési terv a kijelölt vezetői körbe javasolt személy vonatkozásában tartalmazza

a) a nevét,

b) a beosztását,

c) a zárt katonai információs rendszeren, illetve mobiltelefonon való elérhetőségét,

d) annak jelölését, ha kizárólag riasztás esetén értesítendő, továbbá

e) az egyéb szükséges megjegyzést.

3. Az azonnali beszámolás módjai, azonosítása és tartalma

9. § Ezen utasítás alkalmazása során a jelentés vagy riasztás információmegosztását zárt katonai információs rendszeren, üzenetben kell megtenni a jelentési terv alapján.

10. § Az 5. § (3) bekezdése alapján tett riasztást zárt katonai információs rendszer hangalapú szolgáltatása vagy azon való elérhetetlenség esetén a mobiltelefon-szolgáltatás útján is meg kell erősíteni értesítés formájában, az értesítési terv alapján.

11. § A kijelölt vezetői kör hangalapú szolgáltatás útján történő értesítése során, annak sikertelensége esetén az értesítést legalább egyszer meg kell ismételni.

12. § A jelentés és riasztás során a kiberbiztonsági incidensre mindig az egyedi azonosítóval és rövid, jellegére utaló megnevezéssel kell hivatkozni a párhuzamos kiberbiztonsági incidensek pontos megkülönböztetése érdekében.

13. § A jelentés során a zárt katonai információs rendszerben megküldött üzenet a kiberbiztonsági incidensközeli helyzet vonatkozásában tartalmazza

a) a bejelentés időpontját,
b) a kategória szerinti besorolását,
c) a kiberbiztonsági incidensközeli helyzet rövid leírását,
d) a kiberbiztonsági incidensközeli helyzet feltételezett legvalószínűbb – negatív – hatásait az érintett szervezetre,
e) a kiberbiztonsági incidensközeli helyzet érintettségét, hatását és kiterjedését és
f) az érintett szervezet bejelentése alapján a kiberbiztonsági incidensközeli helyzet legveszélyesebb feltételezett kimenetelének megbecslését.

14. § A riasztás során zárt katonai információs rendszerben megküldött üzenet a kiberbiztonsági incidens vonatkozásában a jelentésben foglaltakon felül tartalmazza

a) a kárenyhítés és -hatás csökkentése érdekében megtett és elrendelt kiberbiztonsági incidenskezelési intézkedések rövid tömör összefoglalását és
b) a javaslatot a kijelölt vezetői kör külső kommunikációra történő felkészülésére.

15. § A riasztással összefüggő értesítés során a hangalapú hívás útján közölt információ tartalmazza

a) a bekövetkezés és a bejelentés időpontját, valamint
b) a zárt katonai információs rendszerben megküldött üzenetben szereplő riasztás tényét.

4. Záró rendelkezések

16. § Ez az utasítás a közzétételét követő napon lép hatályba.

17. § A kijelölt vezetői körbe történő első jelölésről a jelen utasítás hatálybalépését követő 8 napon belül intézkedni kell. A felülvizsgálat és a 8. § végrehajtása érdekében végzett adatszolgáltatás a 8. § szerinti szervezet felelőssége.

18. § (1) A Honvédelmi Minisztérium Ügyelet működésének szabályozásáról szóló 66/2021. (XII. 22.) HM utasítás (a továbbiakban: Utasítás1) 1. §-a helyébe a következő rendelkezés lép:

„1. § (1) Az utasítás hatálya a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény (a továbbiakban: Hvt.) 3. § 14. pontja szerinti honvédelmi szervezetre (a továbbiakban: honvédelmi szervezet) terjed ki.

(2) Az utasítást a kijelölt vezetői kör részére történő kiberbiztonsági incidenskezeléssel összefüggő azonnali beszámolás eljárásrendre nem kell alkalmazni.”

(2) Hatályát veszti az Utasítás1 14. § m) pontja.

Szalay-Bobrovniczky Kristóf s. k.,
honvédelmi miniszter

A honvédelmi miniszter 10/2025. (IV. 30.) HM utasítása a duális képzéssel összefüggő feladatokról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontja alapján a következő utasítást adom ki:

1. § Az utasítás hatálya – a Katonai Nemzetbiztonsági Szolgálat kivételével – a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 3. § 14. pontja szerinti honvédelmi szervezetekre terjed ki.

2. § Az utasítás alkalmazásában

1. *szakképzési munkaszerződés:* a szakképzésről szóló 2019. évi LXXX. törvény (a továbbiakban: Szkt.) 83. §-a szerinti munkaszerződés,
2. *szakmai gyakorlóhely:* az a honvédségi szervezet, amely a tanuló, illetve a képzésben részt vevő személy számára a szakképzésről szóló 2019. évi LXXX. törvény végrehajtásáról szóló 12/2020. (II. 7.) Korm. rendelet szerinti szakmai gyakorlatot – az oktatott szakma ágazati besorolásától függetlenül – az Szkt. 100. §-a szerinti területileg illetékes kamara által nyilvántartásba vett duális képzőhelyként biztosítja,
3. *tanuló vagy képzésben részt vevő személy:* szakképző intézményben tanulmányokat folytató és a szakirányú oktatást szakmai gyakorlóhelyen szakképzési munkaszerződéssel teljesítő személy.

3. § (1) A duális képzéssel kapcsolatos feladatellátásra kijelölhető honvédségi szervezetre vonatkozó javaslatot a Honvéd Vezérkar főnöke (a továbbiakban: HVKF) terjeszti fel a Honvédelmi Minisztérium ágazati szakképzésért felelős államtitkára (a továbbiakban: HM szakképzésért felelős államtitkár) részére. A HM szakképzésért felelős államtitkár döntésének tájékoztatására a HVKF intézkedik a kijelölt honvédségi szervezet felé.

(2) A kijelölt honvédségi szervezet a területileg illetékes kamaránál kezdeményezi a szakmai gyakorlóhelyként való nyilvántartásba vételét, amelyről – haladéktalanul, szolgálati úton – értesíti a HM Szervezeti és Működési Szabályzatában a honvédelmi ágazat képzési rendszerének felügyeletére, monitorozására kijelölt szervezeti egységét (a továbbiakban: a HM szakmai szervezeti egység).

(3) A szakmai gyakorlóhelyként nyilvántartásba vett honvédségi szervezet a nyilvántartásba vételről és esetlegesen a nyilvántartott adatokban bekövetkezett változásról – az Szkt. 100. §-a szerinti területileg illetékes kamarának történő bejelentéssel egyidejűleg – köteles szolgálati úton értesíteni a HM szakmai szervezeti egységet.

(4) A szakmai gyakorlóhely a honvédelem ágazatba tartozó szakmák befejező évfolyamáról érkező vagy a honvédelemért felelős miniszter fenntartói irányítása alatt álló szakképző intézményben tanuló vagy képzésben részt vevő személy szakmai gyakorlati oktatásának megszervezését a HM szakmai szervezeti egység részére megküldött – a tanuló vagy a képzésben részt vevő személyi adatainak mellőzését tartalmazó – indokolást követően utasíthatja vissza.

4. § A Honvéd Vezérkar által kijelölt szerv tájékoztatást nyújt – a szakmai gyakorlóhely statisztikai adatokon alapuló összegzése alapján – az adott tanév október 1-jéig megkötött szakképzési munkaszerződésekről – az Információ Kapcsolati Rendszeren keresztül, a HM szakmai szervezeti egység útján – a HM szakképzésért felelős államtitkár részére, legkésőbb az adott tanév október 15-éig, az 1. mellékletben foglalt tartalommal.

5. § (1) A szakképzési munkaszerződés alapján létrejövő jogviszonnyal kapcsolatos adatkezeléseket a szakmai gyakorlóhely mint adatkezelő látja el.

(2) Az (1) bekezdés szerinti adatkezelő az adatkezelés megkezdése előtt gondoskodik adatkezelési tájékoztató igazolható módon történő átadásáról. Az adatkezelési tájékoztatót nem kiskorú tanuló vagy képzésben részt vevő személy esetén az érintett, illetve kiskorú tanuló vagy képzésben részt vevő személy esetén a törvényes képviselő részére kell átadni.

(3) Az adatkezelő az adatkezelési tájékoztató megismeréséről és annak tudomásulvételéről nyilatkoztatja a tanulót vagy képzésben részt vevő személyt, illetve a törvényes képviselőt, ha az érintett kiskorú.

6. § Ez az utasítás a közzétételét követő napon lép hatályba.

7. § A HVKF az utasítás hatálybalépését követő 90 napon belül intézkedik

a) a duális képzéssel kapcsolatos feladatok végrehajtásának részletszabályozásáról,

b) a szakmai gyakorlóhelynél kapcsolattartó kijelöléséről és a kijelölést követő 30 napon belül a kapcsolattartó elérhetőségének a HM szakmai szervezeti egység részére történő megküldéséről.

Szalay-Bobrovniczky Kristóf s. k.,
honvédelmi miniszter

1. melléklet a 10/2025. (IV. 30.) HM utasításhoz

ADATSZOLGÁLTATÁS
szakképzési munkaszerződés megkötéséről

Sorszám	Szakmai gyakorlóhely megnevezése	Szakképzési munkaszerződésben szereplő szakma megnevezése	Szakképzési munkaszerződés kezdete (év/hó/nap)	Szakképzési munkaszerződés vége (év/hó/nap)	18 év alatti személy (I/N)

A honvédelmi miniszter 11/2025. (IV. 30.) HM utasítása a belföldi reprezentációról szóló 20/2020. (IV. 20.) HM utasítás módosításáról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontja alapján a következő utasítást adom ki:

1. § A belföldi reprezentációról szóló 20/2020. (IV. 20.) HM utasítás (a továbbiakban: Ut.) a következő 13. §-sal egészül ki:
„13. § Ezen utasításnak a belföldi reprezentációról szóló 20/2020. (IV. 20.) HM utasítás módosításáról szóló 11/2025. (IV. 30.) HM utasítással módosított 1. mellékletét 2025. január 1-jétől kell alkalmazni.”

2. § Az Ut. 1. melléklete az 1. melléklet szerint módosul.

3. § Ez az utasítás a közzétételét követő napon lép hatályba.

Szalay-Bobrovniczky Kristóf s. k.,
honvédelmi miniszter

1. melléklet a 11/2025. (IV. 30.) HM utasításhoz

1. A belföldi reprezentációról szóló 20/2020. (IV. 20.) HM utasítás (a továbbiakban: Ut.) 1. mellékletében foglalt táblázat
   a) A:5 mezőjében a „KNBSZ igazgató (főigazgató-helyettes)" szövegrész helyébe a „KNBSZ főnök (főigazgató-helyettes)" szöveg és
   b) A:6 mezőjében a „KNBSZ titkárságvezető" szövegrész helyébe a „KNBSZ igazgató (felderítő csoportfőnök)" szöveg
   lép.

2. Hatályát veszti az Ut. 1. mellékletében foglalt táblázat A:6 mezőjében a „KNBSZ főosztályvezető" szövegrész.

A honvédelmi miniszter 12/2025. (IV. 30.) HM utasítása az ügyeletes minisztériumi felsővezetői feladatok ellátásáról és a jelentési kötelezettség körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről szóló 2/2020. (I. 24.) HM utasítás és a Honvédelmi Minisztérium és a miniszter közvetlen alárendeltségébe tartozó szervezetek ügyeleti és készenléti szolgálatairól szóló 34/2021. (VII. 23.) HM utasítás módosításáról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontja alapján a következő utasítást adom ki:

1. Az ügyeletes minisztériumi felsővezetői feladatok ellátásáról és a jelentési kötelezettség körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről szóló 2/2020. (I. 24.) HM utasítás módosítása

1. § Az ügyeletes minisztériumi felsővezetői feladatok ellátásáról és a jelentési kötelezettség körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről szóló 2/2020. (I. 24.) HM utasítás (a továbbiakban: HM utasítás1) 3. § (6) bekezdése helyébe a következő rendelkezés lép:

„(6) Az ügyeletes minisztériumi felsővezetői feladatokat ellátó politikai vagy szakmai felsővezetők heti váltásonkénti beosztását havonta a HM Közigazgatási Államtitkári Titkárság a tárgyhónapot megelőző hónap 20. napjáig állítja össze, és megküldi a HM Ü, valamint a HM Védelmi Igazgatási Főosztály részére. A HM Ü a tárgyhónapot megelőző hónap 23. napjáig megküldi az ügyeletes minisztériumi felsővezetők tárgyhavi beosztását a Kormányügyeletnek."

2. § A HM utasítás1
   a) 3. § (1) bekezdésében a „Kormányügyelet" szövegrész helyébe a „rendészetért felelős miniszter által vezetett minisztérium ügyeleti feladatokat ellátó szerve (a továbbiakban: Kormányügyelet)" szöveg,
   b) 4. § b) pont ba) alpontjában a „NATO válságreagálási rendszerével" szövegrész helyébe a „NATO Reagáló Rendszerével" szöveg,
   c) 4. § e) pontjában az „olyan előre" szövegrész helyébe az „olyan, előre" szöveg
   lép.

2. A Honvédelmi Minisztérium és a miniszter közvetlen alárendeltségébe tartozó szervezetek ügyeleti és készenléti szolgálatairól szóló 34/2021. (VII. 23.) HM utasítás módosítása

3. § A Honvédelmi Minisztérium és a miniszter közvetlen alárendeltségébe tartozó szervezetek ügyeleti és készenléti szolgálatairól szóló 34/2021. (VII. 23.) HM utasítás (a továbbiakban: HM utasítás2) 4. §-a a következő b) ponttal egészül ki:

(Készenléti szolgálatok:)

„b) Ügyeletes Minisztériumi Felsővezető (a továbbiakban: ÜMFV),"

4. § A HM utasítás2 7. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A miniszter, a HM parlamenti államtitkár, a HM közigazgatási államtitkár (a továbbiakban: HM KÁT), a HM haderőfejlesztésért és védelempolitikáért felelős államtitkár, a HM sportért felelős államtitkár, a HM katonai nemzetbiztonság irányításáért felelős államtitkár, a helyettes államtitkárok, a HVKF, a Miniszteri Kabinet kabinetfőnöke, valamint a HM Szervezeti és Működési Szabályzatáról szóló HM utasítás szerinti HM önálló szervezeti egységek vezetői által kijelölt ügyintézők vagy ügyeleti szolgálatok munkanapokon, a hivatali munkaidő utolsó órájában, tájékoztatják a HM Ü-t a bekezdésben meghatározott vezetők munkaidőn túli elérhetőségéről."

5. § A HM utasítás2 a következő 8. alcímmel egészül ki:

„8. Ügyeletes Minisztériumi Felsővezető

12. § (1) Az ÜMFV kiemelt feladata, hogy a kormányügyeleti rendszer részeként, a miniszter felelőségi körébe tartozó és kormányzati intézkedést igénylő rendkívüli események vonatkozásában a Kormányt gyorsan, hatékonyan és hitelesen tájékoztassa.

(2) AZ ÜMFV-i feladatok ellátására az ügyeletes minisztériumi felsővezetői feladatok ellátásáról és a jelentési kötelezettség körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről szóló 2/2020. (I. 24.) HM utasítást kell alkalmazni.

(3) Az ÜMFV kizárólag közvetlenül a miniszter alárendeltségébe tartozik.

(4) Az ÜMFV irányítási jogkört gyakorol a HM Ü felett, annak biztonsági ügyeleti feladatainak ellátásával kapcsolatban.

(5) A szolgálat ellátásával összefüggő követelményeket – különösen a szolgálat feladatait, a szolgálatot adó személyek eligazításának és felkészülésének rendjét, tartózkodási helyét, készenlétét, riasztását és kiértesítését, szolgálati helyre történő beérkezését, valamint a Kormányügyelet tájékoztatásának körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékét – a HM KÁT az ÜMFV-i feladatok ellátásához kiadott Segédletben határozza meg."

6. § (1) A HM utasítás2 21. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A HM meghatározott állományának riasztása, kiértesítése, berendelése és készenléti, illetve ügyeleti szolgálatba helyezése, továbbá egyéb riasztási feladatok végrehajtása érdekében a HM KÁT Titkárság, továbbá a helyettes államtitkári titkárságok – a HM Sportért Felelős Államtitkár alárendeltségébe tartozók kivételével – irányításával, a HM KÁT, továbbá az adott helyettes államtitkár közvetlen alárendeltségébe tartozó főosztályok összevont személyi állományából, heti váltással, egy-egy fő RÉKSZ-et lát el."

(2) A HM utasítás2 21. § (5) bekezdése helyébe a következő rendelkezés lép:

„(5) A HM állományába tartozó szolgálatot ellátók névjegyzékét az adott HM szervezeti egység vezetője, az MH állományába tartozó szolgálatot ellátók névjegyzékét az állományilletékes parancsnok hagyja jóvá."

7. § A HM utasítás2 22. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) A SOKSZ-ot a HM VIF Speciális Objektumok Osztály állományából egy fő hivatásos vagy szerződéses állományú katona heti váltásban látja el."

8. § A HM utasítás2 a következő 26. §-sal egészül ki:

„26. § Az utasítás hatálybalépését követő 30 napon belül a HM VIF gondoskodik a 12. § (5) bekezdése szerinti Segédlet kiadásáról."

3. Záró rendelkezések

9. § Ez az utasítás a közzétételét követő napon lép hatályba.

Szalay-Bobrovniczky Kristóf s. k.,
honvédelmi miniszter

A nemzetgazdasági miniszter 17/2025. (IV. 30.) NGM utasítása a Nemzetgazdasági Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2024. (XII. 30.) NGM utasítás módosításáról

A kormányzati igazgatásról szóló 2018. évi CXXV. törvény 19. § (4) bekezdésében meghatározott hatáskörömben eljárva, a jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontjában foglaltakra figyelemmel – a miniszterelnök jóváhagyásával – a következő utasítást adom ki:

1. § A Nemzetgazdasági Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2024. (XII. 30.) NGM utasítás (a továbbiakban: SzMSz) 1. melléklete az 1. melléklet szerint módosul.

2. § (1) Az SzMSz 1. függeléke helyébe az 1. függelék lép.
(2) Az SzMSz 2. függeléke a 2. függelék szerint módosul.
(3) Az SzMSz 3. függeléke a 3. függelék szerint módosul.
(4) Az SzMSz 4. függeléke a 4. függelék szerint módosul.

3. § Ez az utasítás a közzétételét követő napon lép hatályba.

Nagy Márton István s. k.,
nemzetgazdasági miniszter

Jóváhagyom:

Orbán Viktor s. k.,
miniszterelnök

1. melléklet a 17/2025. (IV. 30.) NGM utasításhoz

1. § Az SzMSz 1. melléklet 6. § d) pontja helyébe a következő rendelkezés lép:
(A miniszter irányítja)
„d) kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár,"
(tevékenységét.)

2. § Az SzMSz 1. melléklet 9. § d) pontja helyébe a következő rendelkezés lép:
(A minisztériumban)
„d) kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár,"
(működik, akiknek tevékenységét a miniszter irányítja.)

3. § Az SzMSz 1. melléklet 18. § (5) bekezdés b) pontja helyébe a következő rendelkezés lép:
(A gazdaságfejlesztésért és iparért felelős államtitkár irányítja)
„b) a stratégiai tranzakciókért felelős helyettes államtitkár,"
(tevékenységét.)

4. § Az SzMSz 1. melléklet 7. alcíme helyébe a következő alcím lép:
„7. A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár
21. § (1) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár
a) ellátja a miniszter vállalkozásfejlesztésért, technológiáért és űriparért való felelősségével kapcsolatos feladatokat,
b) gondoskodik a vállalkozásfejlesztéshez kapcsolódó jogszabályok, közjogi szervezetszabályozó eszközök és kormányzati döntések, továbbá e tárgykörökben felhatalmazás alapján miniszteri rendeletek előkészítéséről,
c) meghatározza a vállalkozásfejlesztéshez kapcsolódó stratégiákat, fejlesztési programokat, és ellátja az azokkal kapcsolatos feladatokat és a programok koordinációját,

d) a stratégiailag fontos vállalati szegmensekkel kapcsolatos felelőssége körében programokat dolgoz ki a hazai gazdasági életben kiemelt jelentőséget betöltő vállalkozások, különösen a magyar tulajdonosi hátterű vállalkozások gazdasági helyzetének megerősítése, regionális versenyképességének fokozása érdekében, valamint kapcsolatot tart ezekkel a vállalkozásokkal,

e) folyamatosan figyelemmel kíséri és elemzi a vállalkozásfejlesztés szempontjából meghatározó gazdasági folyamatokat, a gazdaságpolitikai programok végrehajtására javasolt intézkedések gazdaságfejlesztési és a hazai vállalkozásokra gyakorolt hatásait,

f) gondoskodik az ESG-hez kapcsolódó jogszabályok előkészítéséről és a vállalkozások ESG-vel kapcsolatos kötelezettségeik ellátását megalapozó eszközrendszer működtetéséről; valamint együttműködik a témában a Szabályozott Tevékenységek Felügyeleti Hatósággal,

g) ellátja a 4. függelék szerint hatáskörébe utalt gazdasági társaságok tevékenységét érintő kötelezettségvállalást nem tartalmazó nemzetközi megállapodások, nyilatkozatok aláírásával, végrehajtásával kapcsolatos feladatokat,

h) előkészíti és végrehajtja a szakmai felügyelete alá tartozó gazdasági társaságok tekintetében a Kormány vagyongazdálkodási politikáját, a szakmai felügyelete alá tartozó gazdasági társaságok, intézmények és egyéb szervezetek létrehozására, átalakítására, valamint megszüntetésére vonatkozó döntéseket, ebben a körben szakmailag előkészíti a kormányzati döntéseket,

i) irányítja és ellenőrzi a szakmai felügyelete alá tartozó gazdasági társaságok gazdálkodását, üzemeltetési, ingatlanfejlesztési és informatikai feladatait,

j) együttműködik az illetékes ágazati államtitkárokkal, a Miniszteri Kabinettel, a Miniszteri Koordinációs és Igazgatási Főosztállyal, valamint feladatkörében kapcsolatot tart az egyéb állami vezetőkkel,

k) kapcsolatot tart a vállalkozási érdekvédelmi szervekkel és kamarákkal,

l) ellátja a vállalkozások védelmével, az üzleti környezetük javításával kapcsolatos feladatokat.

(2) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár technológiával és védelmi iparral kapcsolatos felelőssége körében

a) a minisztérium gazdaságfejlesztési, iparügyi és űriparfejlesztési stratégiájához, feladataihoz alapvetően igazodva, azokat támogatva, más minisztériumok ágazati szakterületeivel együttműködésben kidolgozza az egyes ágazatokat érintő technológiai fejlesztési javaslatokat, valamint szolgáltatási stratégiát, ehhez kapcsolódó programok kidolgozására tesz javaslatot, illetve koordinálja e programok végrehajtását,

b) koordinálja és előkészíti az a) ponthoz kapcsolódó, valamint a gazdaság emelt szintű digitalizációját, az élvonalbeli, feltörekvő (digitális) technológiák átvételét támogató, illetve az információs és kommunikációs technológiák iparág (a továbbiakban: IKT iparág) fejlesztését célzó programok, intézkedések kidolgozását, illetve felügyeli e programok végrehajtását, és nyomon követi megvalósításukat a nemzetközi versenyképesség biztosítása érdekében,

c) felel a védelmi ipari fejlesztésekért és beruházásokért.

(3) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár az űriparfejlesztésért és űrtechnológiákért való felelőssége körében

a) felügyeli az európai uniós tagsággal összefüggő és más nemzetközi feladatok ellátását, továbbá gondoskodik az ehhez szükséges hazai jogalkotási feladatok megvalósításáról,

b) felel az űrkutatáshoz és űrtevékenységhez kapcsolódó szabályozásért (különös tekintettel az európai uniós irányelvek érvényesítésére), az ehhez szükséges kormányzati döntések előkészítéséért, valamint működésének fejlesztéséért (különös tekintettel a kapcsolódó stratégiák kidolgozására és a kapcsolódó programok meghatározására, a végrehajtás feltételeinek megteremtésére),

c) ellátja az űriparfejlesztéssel kapcsolatos feladatokat, ideértve különösen a műholdak és a hozzájuk tartozó földi egységek fejlesztésével, kiépítésével, működtetésével és az ezekhez kapcsolódó szolgáltatásokkal összefüggő feladatokat, az űripari ökoszisztémával kapcsolatos tevékenységet, valamint részt vesz az európai uniós és nemzetközi szervezetekben a minisztériummal összefüggő feladatokban.

(4) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár meghatározza a belgazdaság irányításának cél-, eszköz- és intézményrendszerét.

(5) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár irányítja

a) a kis- és középvállalkozások fejlesztéséért felelős helyettes államtitkár,

b) a technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár, valamint

c) a vállalkozások védelméért felelős helyettes államtitkár

tevékenységét.

22. § (1) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár munkájának és feladatainak ellátását kabinet segíti.
(2) A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár irányítja kabinetfőnökének tevékenységét.
23. § A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár – ha nem a minisztert helyettesítő jogkörében jár el – akadályoztatása vagy távolléte esetén a kis- és középvállalkozások fejlesztéséért felelős helyettes államtitkár, együttes akadályoztatásuk vagy távollétük esetén a technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár helyettesíti. A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár hatáskörét a tisztség betöltetlensége esetén a kis- és középvállalkozások fejlesztéséért felelős helyettes államtitkár gyakorolja."

5. § Az SzMSz 1. melléklet 37. § b) pontja helyébe a következő rendelkezés lép:
(A minisztériumban)
„b) stratégiai tranzakciókért felelős helyettes államtitkár,"
(működik.)

6. § Az SzMSz 1. melléklet 37. § l) pontja helyébe a következő rendelkezés lép:
(A minisztériumban)
„l) technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár,"
(működik.)

7. § Az SzMSz 1. melléklet 16. alcíme helyébe a következő alcím lép:
„16. A stratégiai tranzakciókért felelős helyettes államtitkár
41. § (1) A stratégiai tranzakciókért felelős helyettes államtitkár stratégiai tranzakciókért való felelőssége körében
a) gondoskodik – az iparügyekért felelős helyettes államtitkárral és a nemzetközi pénzügyi kapcsolatokért és kifektetéspolitikáért felelős helyettes államtitkárral együttműködve – a Kormány döntéséből fakadó stratégiai célú tranzakciós ügyletek koncepciójának kidolgozásáról, továbbá koordinálja és felügyeli azok végrehajtását,
b) javaslatot tesz a gazdaságfejlesztési célokkal összhangban álló potenciális tranzakciók feltérképezésére,
c) a Kormány felhatalmazása alapján gondoskodik az állami vagyonelemek értékeléséről és szükség esetén javaslatot tesz annak stratégiai átalakítására,
d) ellátja a kormányzati döntések előkészítésével kapcsolatos feladatokat,
e) szervezi és felügyeli az irányítása alá tartozó szervezeti egységek által végzett tevékenységet,
f) a Kormány döntése alapján megvizsgálja az állami tulajdonba bevonni tervezett vagyonelemeket,
g) képviseli a minisztériumot a Kormány által megállapított módon és rendben, a miniszter megbízása és utasítása szerint,
h) előkészíti a koncesszióra vonatkozó kormányzati döntéseket,
i) ellátja a miniszter hatáskörébe tartozó koncessziós szerződések teljesítéséből, végrehajtásából eredő feladatok Nemzeti Koncessziós Iroda (a továbbiakban: NKOI) bevonásával történő előkészítését.
(2) A stratégiai tranzakciókért felelős helyettes államtitkár irányítja
a) az Átvilágításokért Felelős Főosztály, valamint
b) a Projektértékelésért Felelős Főosztály
vezetőjének tevékenységét.
42. § (1) A stratégiai tranzakciókért felelős helyettes államtitkár feladatellátásának támogatása érdekében titkárság működik.
(2) A stratégiai tranzakciókért felelős helyettes államtitkár irányítja titkársága vezetőjének tevékenységét.
43. § A stratégiai tranzakciókért felelős helyettes államtitkárt akadályoztatása, távolléte esetén a nemzetközi pénzügyi kapcsolatokért és kifektetéspolitikáért felelős helyettes államtitkár helyettesíti. A stratégiai tranzakciókért felelős helyettes államtitkár hatáskörét a tisztség betöltetlensége esetén a gazdaságfejlesztésért és iparért felelős államtitkár gyakorolja."

8. § Az SzMSz 1. melléklet 26. alcíme helyébe a következő alcím lép:
„26. Technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár
72. § (1) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár a minisztérium gazdaságfejlesztési, iparügyi és űriparfejlesztési stratégiájához, feladataihoz alapvetően igazodva, azokat

támogatva, más minisztériumok ágazati szakterületeivel együttműködésben kidolgozza az egyes ágazatokat érintő technológiai fejlesztési javaslatokat, valamint szolgáltatási stratégiát, javaslatot tesz az ehhez kapcsolódó programok kidolgozására, illetve koordinálja e programok végrehajtását.

(2) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár ellátja az űriparfejlesztéssel és űrtechnológiákkal összefüggő feladatokat, űripari tárgyú programokat tervez és hajt végre, képviseli a Kormányt az űripari vonatkozású nemzetközi szervezetekben, így különösen, de nem kizárólagosan az Európai Űrügynökségben és az Európai Unió Űrprogramügynökségében, felel a nemzeti delegációk összeállításáért, koordinálja és vezeti munkájukat.

(3) Kidolgozza a védelmi ipari stratégiát, irányítja a stratégia végrehajtását, valamint koordinálja a védelmi ipari fejlesztéseket és beruházásokat.

(4) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár az (1) bekezdés szerinti feladatai keretében

a) a minisztérium ipari felelősségének keretében irányítja a hazai IKT iparág fejlesztési programok előkészítését, valamint koordinálja azok végrehajtását,

b) a foglalkoztatásért és programokért felelős helyettes államtitkárral együttműködve gondoskodik az új technológiák használatához kapcsolódó kompetenciafejlesztési programok előkészítéséről és végrehajtásáról,

c) felel egyes kiemelt technológiák alkalmazása előtti szabályozási akadályok elhárításáért, a technológiák használatát támogató szabályozási környezet megteremtéséért,

d) más szakterületek által készített, az ágazatok infokommunikációs tartalmú, valamint egyéb, technológiával kapcsolatos előterjesztéseiről, programjairól véleményt nyilvánít, egyetértési jogot gyakorol és javaslatot tesz a miniszter felé,

e) előzetesen véleményezi a minisztérium tulajdonosi joggyakorlása alá tartozó gazdasági társaságok, valamint a minisztérium által irányított költségvetési szervek ágazati technológiai fejlesztéseit, miniszteri utasításban szabályozott esetekben jóváhagyja, ennek érdekében informatikai rendszert működtet,

f) irányítja a Nemzeti Technológiai Platform tevékenységét,

g) szakmai irányítást gyakorol a Neumann János Nonprofit Korlátolt Felelősségű Társaság felett,

h) a Neumann János Nonprofit Korlátolt Felelősségű Társaság útján gondoskodik egyes kiemelt technológiák ökoszisztémájának fejlesztését biztosító platformok, illetve koalíciók működési feltételeinek megteremtéséről, különös tekintettel az 5G, a Mesterséges Intelligencia, a drón-, a blockchain-, valamint az Ipar 4.0 technológiákra, gondoskodik továbbá a magyarországi félvezető ökoszisztéma fejlesztését elősegítő stratégia és zászlóshajó projektek kidolgozásáról és azok végrehajtásáról,

i) koordinálja egyes kiemelt technológiák ágazati alkalmazását biztosító pilot programok lebonyolítását,

ia) hozzájárul a diszruptív és kettős felhasználású technológiák ágazati alkalmazásához, részt vesz a védelmi digitalizációs kezdeményezések kidolgozásában és megvalósításában,

ib) közreműködik Magyarország Nemzeti Kiberbiztonsági Stratégiájának kidolgozásában és végrehajtásában, a Neumann János Nonprofit Korlátolt Felelősségű Társaság útján részt vesz a vállalatok biztonsági tudatosságának fejlesztésében, rezilienciájuk erősítésében,

j) gondoskodik az ágazatok szuperszámítógép-felhasználási igényeinek kielégítéséről saját, vagy a nemzeti HPC kompetencia központ által üzemeltetett infrastruktúra útján,

k) koordinálja a hazai kvantumszámítás-technikai tevékenységet,

ka) a mesterséges intelligencia e-közigazgatásban való alkalmazásának kivételével előkészíti a mesterséges intelligenciával összefüggő szabályozási javaslatokat, és gondoskodik a mesterséges intelligenciával foglalkozó Európai Uniós és nemzetközi szervezetekben való részvételről,

kb) ellátja a Kormány képviseletét a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet) szóló, 2024. június 13-i (EU) 2024/1689 európai parlamenti és tanácsi rendelet (a továbbiakban: MI Rendelet) szerinti Mesterséges Intelligenciával Foglalkozó Európai Testületben,

l) felelősként vagy közreműködőként gondoskodik a hatáskörébe tartozó, a 2021–2027 közötti európai uniós tervezési időszak konstrukcióinak szakmai előkészítéséről, részt vesz a programok értékelési és monitoring tevékenységében,

m) részt vesz szavazó jogú tagként a minisztérium képviseletében a DIMOP Plusz Monitoring Bizottságokban,

n) az e bekezdés szerinti feladatai ellátása során gondoskodik az informatikáért felelős miniszterrel való szakmai együttműködés koordinációjáról.

(5) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár a (2) bekezdés szerinti feladatai keretében

a) gondoskodik az űriparfejlesztéssel és űrtechnológiákkal összefüggő szabályozás előkészítéséről,

b) gondoskodik az űriparfejlesztéssel és űrtechnológiákkal összefüggő stratégiai tervezésről és e stratégiák végrehajtásáról,

c) gondoskodik a Kormány képviseletének biztosításáról az űriparfejlesztéssel és űrtechnológiákkal összefüggő európai uniós és nemzetközi szervezetekben (ideértve különösen az Európai Űrügynökséget és az Európai Unió Űrprogramügynökségét),

d) gondoskodik az űripari ökoszisztémával kapcsolatos fejlesztésről,

e) ellátja a hazai műholdas infrastruktúra fejlesztésével, kiépítésével és működtetésével összefüggő kormányzati feladatokat,

f) kidolgozza a hazai űripari tevékenységgel összefüggő kormányzati feladatok ügynökségi rendszerben történő ellátására vonatkozó javaslatot.

(6) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár a (3) bekezdés szerinti feladatainak keretében

a) az érintett minisztériumok bevonásával javaslatot tesz a védelmi iparfejlesztés stratégiai irányaira, és ellátja a kormányközi koordinációt,

b) javaslatot tesz a védelmi ipari termékek és szolgáltatások hazai és nemzetközi piacra jutásának stratégiájával kapcsolatosan,

c) a védelmi iparfejlesztés stratégia előmozdítása érdekében előkészíti, kezdeményezi a védelmi ipari stratégiai együttműködéseket,

d) végrehajtja a védelmi ipari beruházások megvalósításával kapcsolatos feladatokat, és koordinálja a védelmi ipari feladatok végrehajtásának rendszerét,

e) kormányzati szinten összehangolja a védelmi ipari állami infrastruktúra-beruházások előkészítését és megvalósítását,

f) koordinálja a védelmi ipari beszállító-fejlesztési program végrehajtásának rendszerét, gondoskodik annak fenntartásáról és finanszírozásáról, valamint javaslatot tesz a forráskezelési és közvetítői feladatok ellátásával kapcsolatosan,

g) szakmai irányítást gyakorol az N7 Nemzeti Védelmi Ipari Innovációs Holding Zártkörűen Működő Részvénytársaság felett,

h) szakmai irányítást gyakorol a Magyar Védelmi Exportügynökség Zártkörűen Működő Részvénytársaság felett.

73. § A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár irányítja

a) a Technológiai Szakpolitikák Fejlesztéséért Felelős Főosztály,

b) a Technológiai Adaptációért és Szabályozásért Felelős Főosztály,

c) az Űrpolitikáért és Űrtevékenységért Felelős Főosztály,

d) a Védelmi Ipar Fejlesztési Főosztály, valamint

e) a Nemzetközi Védelmi Ipari Együttműködési Főosztály

vezetőjének tevékenységét.

74. § (1) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár feladatainak ellátása érdekében titkárság működik.

(2) A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár irányítja a titkársága vezetőjének tevékenységét.

75. § A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár akadályoztatása vagy távolléte esetén a helyettesítésre az alábbi sorrendben kerül sor: Űrpolitikáért és Űrtevékenységért Felelős Főosztály vezetője, a Technológiai Adaptációért és Szabályozásért Felelős Főosztály vezetője, a Védelmi Ipar Fejlesztési Főosztály vezetője, valamint a Nemzetközi Védelmi Ipari Együttműködési Főosztály vezetője, együttes távollétük vagy akadályoztatásuk esetén a Technológiai Szakpolitikák Fejlesztéséért Felelős Főosztály vezetője. A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár hatáskörét a tisztség betöltetlensége esetén az Űrpolitikáért és Űrtevékenységért Felelős Főosztály vezetője gyakorolja.”

9. § Az SzMSz 1. melléklet 76. § (1) bekezdés a) pontja helyébe a következő rendelkezés lép:

(A kis- és középvállalkozások fejlesztéséért felelős helyettes államtitkár)

„a) gondoskodik – a nemzetközi pénzügyi kapcsolatokért és kifektetéspolitikáért felelős helyettes államtitkárral, a fogyasztóvédelemért és kereskedelemért felelős helyettes államtitkárral, az iparügyekért felelős helyettes

államtitkárral, valamint a technológiáért, űriparért és védelmi iparért felelős helyettes államtitkárral együttműködve – a Statútum 111/E. §-a szerinti vállalkozások fejlesztésével kapcsolatos stratégiák, koncepciók, intézkedések kidolgozásáról, továbbá koordinálja és felügyeli ezek végrehajtását,"

10. § Az SzMSz 1. melléklete a következő 141. §-sal egészül ki:

„141. § A Szabályzatnak a Nemzetgazdasági Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2024. (XII. 30.) NGM utasítás módosításáról szóló 17/2025. (IV. 30.) NGM utasítással megállapított 6. § d) pontját, 9. § d) pontját, 18. § (5) bekezdés b) pontját, 7. alcímét, 37. § b) pontját, 37. § l) pontját, 16. alcímét, 26. alcímét, 76. § (1) bekezdését, az 1. függelékét, a 2. függelék 2.1.0.2. pont a) alpont 1. pontját, 2. függelék 2.2.2. alcímét, 2. függelék 2.2.2.1. pontját, 2. függelék 2.4. alcímét, 2. függelék 2.4.0.1. pontját, 2. függelék 2.4.1 alcím címét, 2. függelék 2.4.1.1. pontját, 2. függelék 2.4.1.5–2.4.1.6. alpontját, a 4. függelék II. Gazdasági társaságok című táblázat 9., 17–18. és 23. sorát, valamint módosított 3. függelékében foglalt táblázatát 2025. április 18. napjától kell alkalmazni, a Szabályzat 18. § (1) bekezdés 28. pontját, a 2. függelék 2.2.2.4. és 2.2.2.5. pontját 2025. április 18. napjától nem kell alkalmazni."

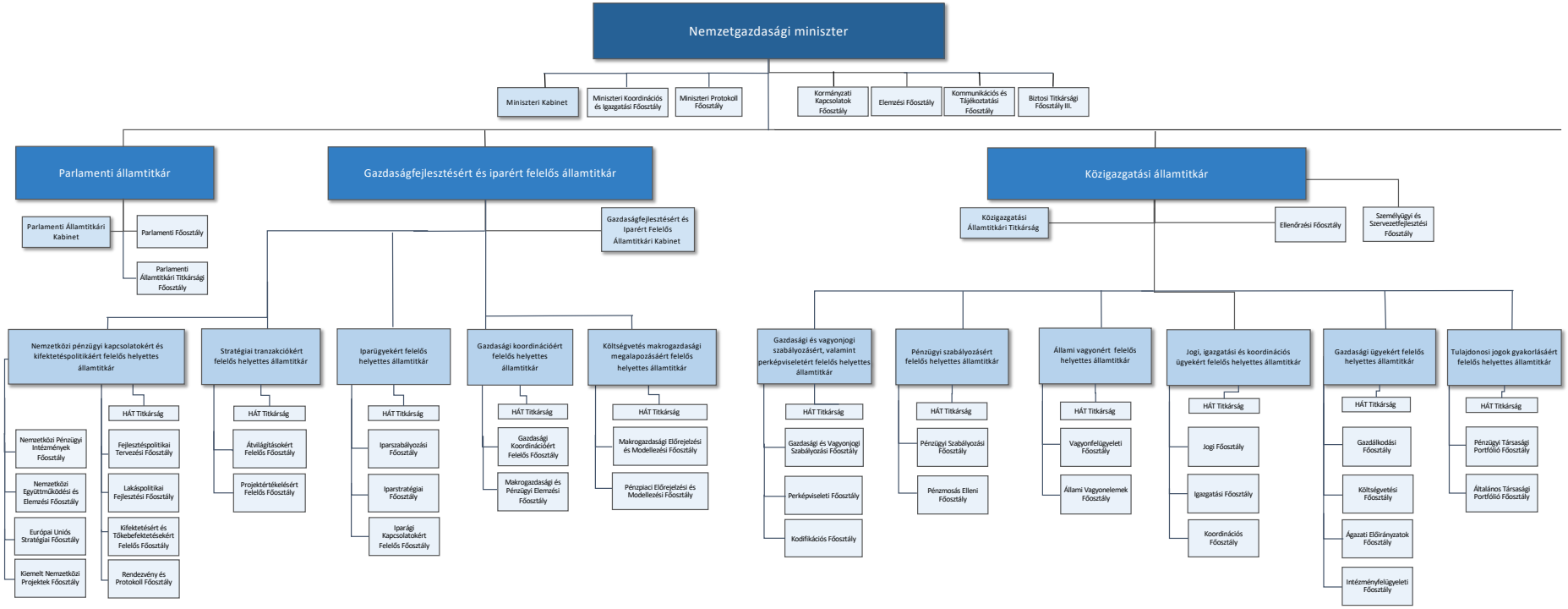
11. § Hatályát veszti az SzMSz 1. melléklet

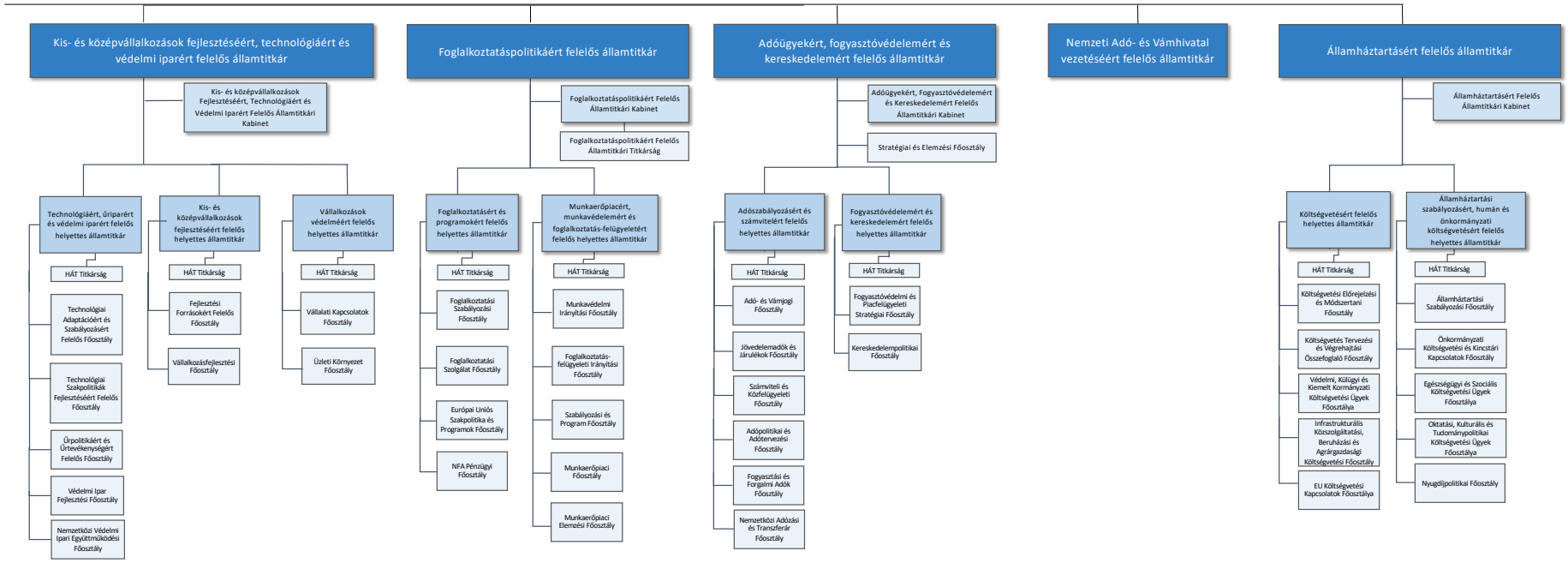
a) 6. § o) pontja,

b) 18. § (1) bekezdés 28. pontja.

1. függelék a 17/2025. (IV. 30.) NGM utasításhoz
„1. függelék

A Nemzetgazdasági Minisztérium szervezeti felépítése




Kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár
Kis- és középvállalkozások Fejlesztéséért, Technológiáért és Védelmi Iparért Felelős Államtitkári Kabinet
Technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár
HÁT Titkárság
Technológiai Adaptációért és Szabályozásért Felelős Főosztály
Technológiai Szakpolitikák Fejlesztéséért Felelős Főosztály
Űrpolitikáért és Űrtevékenységért Felelős Főosztály
Védelmi Ipar Fejlesztési Főosztály
Nemzetközi Védelmi Ipari Együttműködési Főosztály
Kis- és középvállalkozások fejlesztéséért felelős helyettes államtitkár
HÁT Titkárság
Fejlesztési Forrásokért Felelős Főosztály
Vállalkozásfejlesztési Főosztály
Vállalkozások védelméért felelős helyettes államtitkár
HÁT Titkárság
Vállalati Kapcsolatok Főosztály
Üzleti Környezet Főosztály
Foglalkoztatáspolitikáért felelős államtitkár
Foglalkoztatáspolitikáért Felelős Államtitkári Kabinet
Foglalkoztatáspolitikáért Felelős Államtitkári Titkárság
Foglalkoztatásért és programokért felelős helyettes államtitkár
HÁT Titkárság
Foglalkoztatási Szabályozási Főosztály
Foglalkoztatási Szolgálat Főosztály
Európai Uniós Szakpolitika és Programok Főosztály
NFA Pénzügyi Főosztály
Munkaerőpiacért, munkavédelemért és foglalkoztatás-felügyeletért felelős helyettes államtitkár
HÁT Titkárság
Munkavédelmi Irányítási Főosztály
Foglalkoztatás-felügyeleti Irányítási Főosztály
Szabályozási és Program Főosztály
Munkaerőpiaci Főosztály
Munkaerőpiaci Elemzési Főosztály
Adóügyekért, fogyasztóvédelemért és kereskedelemért felelős államtitkár
Adóügyekért, Fogyasztóvédelemért és Kereskedelemért Felelős Államtitkári Kabinet
Stratégiai és Elemzési Főosztály
Adószabályozásért és számvitelért felelős helyettes államtitkár
HÁT Titkárság
Adó- és Vámjogi Főosztály
Jövedelemadók és Járulékok Főosztály
Számviteli és Közfelügyeleti Főosztály
Adópolitikai és Adótervezési Főosztály
Fogyasztási és Forgalmi Adók Főosztály
Nemzetközi Adózási és Transzferár Főosztály
Fogyasztóvédelemért és kereskedelemért felelős helyettes államtitkár
HÁT Titkárság
Fogyasztóvédelmi és Piacfelügyeleti Stratégiai Főosztály
Kereskedelempolitikai Főosztály
Nemzeti Adó- és Vámhivatal vezetéséért felelős államtitkár
Államháztartásért felelős államtitkár
Államháztartásért Felelős Államtitkári Kabinet
Költségvetésért felelős helyettes államtitkár
HÁT Titkárság
Költségvetési Előrejelzési és Módszertani Főosztály
Költségvetés Tervezési és Végrehajtási Összefoglaló Főosztály
Védelmi, Külügyi és Kiemelt Kormányzati Költségvetési Ügyek Főosztálya
Infrastrukturális Közszolgáltatási, Beruházási és Agrárgazdasági Költségvetési Főosztály
EU Költségvetési Kapcsolatok Főosztálya
Államháztartási szabályozásért, humán és önkormányzati költségvetésért felelős helyettes államtitkár
HÁT Titkárság
Államháztartási Szabályozási Főosztály
Önkormányzati Költségvetési és Kincstári Kapcsolatok Főosztály
Egészségügyi és Szociális Költségvetési Ügyek Főosztálya
Oktatási, Kulturális és Tudománypolitikai Költségvetési Ügyek Főosztálya
Nyugdíjpolitikai Főosztály

"

2. függelék a 17/2025. (IV. 30.) NGM utasításhoz

1. Az SzMSz 2. függelék 2.1.0.2. pont a) alpont 1. pontja helyébe a következő rendelkezés lép:
(A Parlamenti Főosztály
koordinációs feladatai körében)
„1. felel a miniszter, a parlamenti államtitkár, a gazdaságfejlesztésért és iparért felelős államtitkár, a kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár, a foglalkoztatáspolitikáért felelős államtitkár, az adóügyekért, fogyasztóvédelemért és kereskedelemért felelős államtitkár, a Nemzeti Adó- és Vámhivatal vezetéséért felelős államtitkár, az államháztartásért felelős államtitkár és a közigazgatási államtitkár országgyűlési munkájának segítéséért, az országgyűlési munka előkészítéséért,"

2. Az SzMSz 2. függelék 2.2.2. alcím címe helyébe a következő alcím cím lép:
„2.2.2. A stratégiai tranzakciókért felelős helyettes államtitkár irányítása alá tartozó szervezeti egységek"

3. Az SzMSz 2. függelék 2.2.2.1. pontja helyébe a következő rendelkezés lép:
„2.2.2.1. A Stratégiai Tranzakciókért Felelős Helyettes Államtitkári Titkárság
A Stratégiai Tranzakciókért Felelős Helyettes Államtitkári Titkárság segíti a stratégiai tranzakciókért felelős helyettes államtitkár tevékenységének az ellátását, ennek keretében ellátja az 1. melléklet 100. §-ában rögzített titkársági feladatokat."

4. Az SzMSz 2. függelék 2.4. alcím címe helyébe a következő alcím cím lép:
„2.4. A kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár irányítása alá tartozó szervezeti egységek"

5. Az SzMSz 2. függelék 2.4.0.1. pontja helyébe a következő rendelkezés lép:
„2.4.0.1. Kis- és Középvállalkozások Fejlesztéséért, Technológiáért és Védelmi Iparért Felelős Államtitkári Kabinet
A Kis- és Középvállalkozások Fejlesztéséért, Technológiáért és Védelmi Iparért Felelős Államtitkári Kabinet
a) közreműködik a kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár döntéseinek előkészítésében, az ahhoz szükséges elemzések elvégzésében és koordinálásában, valamint
b) a kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár által felügyelt projektek koordinációjában és az államtitkár által közvetlenül meghatározott feladatok ellátásában."

6. Az SzMSz 2. függelék 2.4.1 alcím címe helyébe a következő alcím cím lép:
„2.4.1. A technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár irányítása alá tartozó szervezeti egységek"

7. Az SzMSz 2. függelék 2.4.1.1. pontja helyébe a következő rendelkezés lép:
„2.4.1.1. Technológiáért, Űriparért és Védelmi Iparért Felelős Helyettes Államtitkári Titkárság
A Technológiáért, Űriparért és Védelmi Iparért Felelős Helyettes Államtitkári Titkárság segíti a technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár tevékenységének az ellátását, ennek keretében ellátja az 1. melléklet 100. §-ában rögzített titkársági feladatokat.
A Technológiáért, Űriparért és Védelmi Iparért Felelős Helyettes Államtitkári Titkárság
a) Adminisztratív feladatai körében
1. előkészítő és adminisztratív feladatokat lát el, rendezi, és jóváhagyásra, aláírásra benyújtja a döntéshozatalra felterjesztett ügyiratokat, illetve illetékesség szerint továbbítja a minisztérium szervezeti egységei és a minisztériumok részére,
2. ellátja a miniszter, a kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár, illetve a technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár által meghatározott egyéb írásos dokumentumok előkészítését.

b) Koordinációs feladatai körében
1. szakmai egyeztetéseket koordinál,
2. döntés-előkészítő anyagokat készít,
3. kapcsolatot tart a minisztérium érintett szervezeti egységeivel és más kormányzati szereplőkkel."

8. Az SzMSz 2. függelék 2.4. alcím 2.4.1. pontja a következő 2.4.1.5–2.4.1.6. alponttal egészül ki:

„2.4.1.5. Védelmi Ipar Fejlesztési Főosztály

A Védelmi Ipar Fejlesztési Főosztály
a) koordinálja a Védelmi Ipari Stratégia és a fejlesztési programok, a Védelmi Ipari Export Stratégia kidolgozását, átdolgozását és végrehajtását,
b) nyomon követi a Védelmi Ipari Stratégia és a kapcsolódó fejlesztési programok, a Védelmi Ipari Export Stratégia végrehajtását, kezdeményezi és koordinálja az azokról szóló kormányzati jelentések elkészítését,
c) közreműködik a Nemzeti Biztonsági Stratégia, a Nemzeti Ellenálló Képesség Stratégia, valamint a védelmi és hadfelszerelési fejlesztésekkel kapcsolatos további stratégiák és programok kidolgozásában,
d) közreműködik az ágazati védelmi tervezési, gazdaságfelkészítési és gazdaságmozgósítási stratégiák, programok és intézkedések kidolgozásában és végrehajtásában,
e) közreműködik a multilaterális védelmi ipari együttműködések kialakításában és hazai feladatainak ellátásában,
f) működteti a védelmi ipari feladatok végrehajtása nyomon követésének rendszerét,
g) felügyeli a védelmi ipari beszállítófejlesztési program végrehajtását és ezzel összefüggésben és ennek részeként a Védelmi Ipari Magántőkealap kezelését és a Védelmi Ipari Beszállító- és Iparfejlesztési Kft. működését,
h) nyomon követi a védelmi ipari fejlesztések minőségbiztosítási és tanúsítási feladataival, valamint a kritikus alapanyagok és alkatrészek készletezésével és kezelésével kapcsolatos hatósági feladatellátás kiépítését és működését,
i) ellátja a gazdaságfelkészítéssel és rögzített védelmi ipari kapacitásokkal kapcsolatos tárcafeladatokat,
j) védelmi ipari beruházási és fejlesztési együttműködéseket kezdeményez, ellátja az ezekhez kapcsolódó előkészítő tevékenységet,
k) koordinálja a védelmi ipari beruházásokkal és fejlesztésekkel kapcsolatos egyéb feladatok kidolgozását és végrehajtását,
l) nyomon követi a védelmi ipari beruházások, fejlesztések és egyéb feladatok gyakorlati megvalósulását és eredményét,
m) koordinálja a közvetlen külföldi védelmi ipari befektetések átvilágításával és engedélyezésével kapcsolatos feladatokat,
n) a hazai haditechnikai célú tevékenység engedélyezési folyamatait érintően együttműködik az engedélyező hatósággal, képviseli a Nemzetgazdasági Minisztériumot a haditechnikai gyártási és exportengedélyek kiadásában és a dual-use munkacsoportban,
o) Védelmi Ipari Adatbázist fejleszt és működtet,
p) részt vesz a hazai védelmi iparral kapcsolatos honvédelmi, rendvédelmi és katasztrófavédelmi beszerzési és kapcsolódó döntések előkészítésében, költségvetési és ipari hatásainak vizsgálatában, ennek érdekében kapcsolatot tart a HM és az MH, a BM és a NAV beszerzés-előkészítő részlegeivel és a Védelmi Beszerzési Ügynökséggel,
q) ellátja a 4. függelék szerint hatáskörébe tartozó gazdasági társaságokat érintő szakmai, gazdasági tárgykörben kiadandó tulajdonosi döntésre benyújtani tervezett előterjesztések, adatszolgáltatások koordinációját, előzetes véleményezését, előkészítését és döntésre való felterjesztését, továbbá felügyeli és ellenőrzi az általa előkészített tulajdonosi döntések végrehajtását,
r) véleményezi az állami tulajdonú ingatlanok védelmi ipari célú hasznosítására vonatkozó javaslatokat,
s) közreműködik a hazai védelmi ipari feladatokat érintő nemzetközi multilaterális és bilaterális feladatokkal kapcsolatos kormányzati álláspont kialakításában és a feladatellátásban, eseti jelleggel részt vesz a kormányközi és gazdasági vegyesbizottságok védelmi ipart érintő munkájában,
t) közreműködik a hazai védelmi kiadások költségvetési tervezésében, nyomon követésében és elemzésében,
u) közvetlen kapcsolattartási és adatkérési jogot gyakorol a feladat- és hatáskörébe tartozó ügyekben a társtárcákkal, a honvédelmi és védelmi szervezetekkel, kormányzati szereplőkkel,
v) kapcsolatot tart és együttműködik a védelmi ipari vállalatokkal és szervezeteikkel: a Magyar Védelemipari Szövetséggel, a Magyar Kereskedelmi és Iparkamarával, a Magyar Bankszövetséggel,
w) közreműködik a jogi szabályozási és a hazai és nemzetközi védelmi ipari együttműködésekkel kapcsolatos kormányzati döntések előkészítésében,

x) előkészíti, illetve véleményezi a Védelmi Tanács és a kormány üléseire benyújtott védelmi ipari vagy azt érintő előterjesztéseket, munkaanyagokat,
y) folyamatosan nyomon követi a 4. függelék szerint hatáskörébe tartozó gazdasági társaságok gazdálkodását, továbbá a tulajdonosi joggyakorlást ellátó szakterülettel együttműködve adatgyűjtést végez, és gondoskodik a kormányzati döntések, állásfoglalások és jogszabályok előkészítéséről,
z) előkészíti, koordinálja és nyilvántartja a szakmai kezelésébe tartozó gazdasági társaságokat érintő támogatásokhoz kapcsolódó döntéseket, a tulajdonosi joggyakorlást ellátó szakterülettel együttműködve ellátja a hatáskörébe tartozó társaságokkal és szervezetekkel való kapcsolattartást, valamint koordinálja és végrehajtja e gazdálkodó szervezetek adataira és információira irányuló adatkéréseket.

2.4.1.6. Nemzetközi Védelmi Ipari Együttműködési Főosztály

A Nemzetközi Védelmi Ipari Együttműködési Főosztály
a) ellátja a magyar kormányzati képviseletet védelmi ipari területen a NATO, az Európai Unió és az Európai Védelmi Ügynökség (European Defence Agency) (a továbbiakban: EDA) és más nemzetközi szervezetek bizottságaiban, munkacsoportjaiban, valamint különböző kezdeményezéseiben,
b) összeállítja a háttér dokumentumokat, kialakítja a magyar nemzeti álláspontot és elkészíti a hozzászólási javaslatot az európai uniós, NATO és EDA döntéshozatalhoz kapcsolódóan védelmi ipari kérdésekben,
c) közreműködik az Európai Tanács Védelmi Ipari Munkacsoportjában (Working Party on Defence Industry, DIWP) képviselendő magyar nemzeti álláspont kidolgozásában és képviseletében,
d) ellátja a multilaterális nemzetközi védelmi ipari megállapodások létrehozásával, módosításával, jóváhagyásával és végrehajtásának nyomon követésével összefüggő feladatokat,
e) közreműködik a NATO és az Európai Unió védelmi iparának megerősítésére irányuló tevékenységek hazai végrehajtásának koordinálásában és nyomon követésében,
f) fogadja a külföldi államoktól és vállalatoktól érkező védelmi ipari tárgyú megkereséseket, igényeket, és végzi az ezekből fakadó hazai feladatokat,
g) szervezi és szakmailag előkészíti a kétoldalú nemzetközi védelmi ipari tárgyalásokat,
h) részt vesz a kétoldalú nemzetközi védelmi ipari technológiai partnerségek létrehozásában, amennyiben szükséges, akkor a kapcsolódó megállapodások, szerződések előkészítésében és végrehajtásuk nyomon követésében,
i) közreműködik védelmi ipari kérdésekben más minisztériumok, különösen a Honvédelmi Minisztérium nemzetközi tárgyalásainak előkészítésében, végrehajtásában és utókövetésében,
j) ellátja a nemzetközi védelmi ipari ügyek társintézményekkel és más szervezetekkel való koordinációját, különösen a HM Hadfelszerelési Főosztállyal, a HVK Haderőtervezési Csoportfőnökséggel, Magyarország brüsszeli NATO melletti Állandó Képviseletének Védelempolitikai Részlegével és Magyarország brüsszeli Európai Unió melletti Állandó Képviseletével,
k) szükség szerint részt vesz – a brüsszeli képviseletekkel együttműködésben – a védelmi miniszteri és nemzeti hadfelszerelési igazgatói szintű üléseken, valamint a Visegrádi Csoport (V4), a Közép-európai Védelmi Együttműködés (Central European Defence Cooperation, CEDC) értekezleteken,
l) felkutatja és elősegíti a hazai védelmi ipar nemzetközi védelmi ipari programokban, projektekben való részvételének lehetőségeit, különösen az Európai Védelmi Ipari Programban (European Defence Industry Programme, EDIP) és annak várható utódprogramjában,
m) felkutatja a hazai védelmi ipar számára a nemzetközi finanszírozási lehetőségeket, és segíti a magyar védelmi ipari szereplőket a hozzájutásban,
n) koordinálja a nemzeti védelmi ipar képviseletét a nemzetközi szervezetekben, különösen a NATO Védelmi Ipari Gyártási Testületben (NATO Defence Industrial Production Board, DIPB) és az EDA munkacsoportjaiban,
o) feladatainak végrehajtása során kapcsolatot tart és együttműködik a NATO Védelmi Beruházási Igazgatóságával (Defence Investment Division, DI), az Európai Bizottság Védelmi Ipari és Űrtevékenységi Főigazgatóságával (Directorate-General for Defence Industry and Space, DG DEFIS), az EDA Ipari Szinergiák és Ösztönzők Igazgatóságával (Industry Synergies & Enablers, ISE) és a NATO Támogató és Beszerzési Ügynökségével (NATO Support and Procurement Agency, NSPA),
p) részt vesz az Európai Koordinációs Tárcaközi Bizottság munkájában, melynek során ellátja a 25.1. Védelmi Ipar és Védelmi Innováció Alcsoport társelnöki és tárcakoordinátori teendőket,
q) végzi a védelmi ipari tartós külszolgálattal kapcsolatos tervezési és koordinációs feladatokat,
r) feladatainak végrehajtása során kapcsolatot tart és együttműködik a minisztérium szervezeti egységeinek vezetőivel, valamint más minisztériumokkal, intézményekkel és egyéb szervezetekkel,

s) részt vesz a kormányközi és gazdasági vegyesbizottságok védelmi ipart érintő munkájában,

t) részt vesz a nemzetközi és hazai védelmi rendezvényeken, konferenciákon és szemináriumokon és bemutatókon,

u) részt vesz a védelmi ipari ágazat hosszú távú stratégiai dokumentumainak kidolgozásában, melynek során javaslatot tesz a nemzetközi védelmi ipari stratégiai együttműködési irányokra és tevékenységekre,

v) védelmi ipari szempontból figyelemmel kíséri a NATO DIANA (Defence Innovation Accelerator for the North Atlantic) és a NATO Innovációs Alap (Innovation Fund), valamint az Európai Védelmi Alap (European Defence Fund, EDF) hazai végrehajtását,

w) elemzi a nemzetközi védelmi ipari helyzetet és tendenciákat, különös tekintettel a NATO és az EU új kezdeményezéseire, melyekről összefoglaló, tájékoztató anyagokat készít."

9. Az SzMSz 2. függelék
   a) 2.2.2.2. pont h) alpontjában a „stratégiai tranzakciókért és védelmi iparért felelős helyettes államtitkár" szövegrész helyébe a „stratégiai tranzakciókért felelős helyettes államtitkár" szöveg,
   b) 2.2.2.3. pont l) alpontjában a „stratégiai tranzakciókért és védelmi iparért felelős helyettes államtitkár" szövegrész helyébe a „stratégiai tranzakciókért felelős helyettes államtitkár" szöveg,
   c) 2.4.1.2. pont c) alpont 7. pontjában a „technológiáért felelős helyettes államtitkár" szövegrész helyébe a „technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár" szöveg,
   d) 2.4.2.1. pont a) alpont 2. pontjában a „kis- és középvállalkozások fejlesztéséért és technológiáért felelős államtitkár" szövegrész helyébe a „kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár" szöveg,
   e) 2.4.3.1. pont a) alpont 2. pontjában a „kis- és középvállalkozások fejlesztéséért és technológiáért felelős államtitkár" szövegrész helyébe a „kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár" szöveg

   lép.

10. Hatályát veszti az SzMSz 2. függelék
    a) 2.2.2.4. pontja,
    b) 2.2.2.5. pontja.

3. függelék a 17/2025. (IV. 30.) NGM utasításhoz

1. Az SzMSz 3. függelékében foglalt táblázat 2.2.2. pontja helyébe a következő pont lép:

(Irányító állami vezető	*Szervezeti egység)*
2.2.2. Stratégiai tranzakciókért felelős helyettes államtitkár	
	2.2.2.1. Stratégiai Tranzakciókért Felelős Helyettes Államtitkári Titkárság
	2.2.2.2. Átvilágításokért Felelős Főosztály
	2.2.2.2.1. Számviteli és Adózási Átvilágításért Felelős Osztály
	2.2.2.2.2. Jogi Átvilágításért Felelős Osztály
	2.2.2.2.3. Üzleti és Technológiai Átvilágításért Felelős Osztály
	2.2.2.3. Projektértékelésért Felelős Főosztály
	2.2.2.3.1. Vételárfelosztásért Felelős Osztály

2. Az SzMSz 3. függelékében foglalt táblázat 2.4. pontja helyébe a következő pont lép:

(Irányító állami vezető	*Szervezeti egység)*
2.4. Kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár	
	2.4.0.1. Kis- és középvállalkozások Fejlesztéséért, Technológiáért és Védelmi Iparért felelős Államtitkári Kabinet

3. Az SzMSz 3. függelékében foglalt táblázat 2.4.1. pontja helyébe a következő pont lép:

(Irányító állami vezető	*Szervezeti egység)*
2.4.1. Technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár	
	2.4.1.1. Technológiáért, Űriparért és Védelmi Iparért Felelős Helyettes Államtitkári Titkárság
	2.4.1.2. Technológiai Adaptációért és Szabályozásért Felelős Főosztály
	2.4.1.2.1. Technológiai Projekttámogatásért Felelős Osztály
	2.4.1.3. Technológiai Szakpolitikák Fejlesztéséért Felelős Főosztály
	2.4.1.3.1. Vállalati Technológiák Osztály
	2.4.1.4. Űrpolitikáért és Űrtevékenységért Felelős Főosztály
	2.4.1.4.1. Űrtevékenység Szabályozásáért és Koordinációért Felelős Osztály
	2.4.1.4.2. Űrpolitikáért és Kiemelt Projektekért Felelős Osztály
	2.4.1.5. Védelmi Ipar Fejlesztési Főosztály
	2.4.1.5.1. Szakpolitikai Stratégiai és Tervezési Osztály
	2.4.1.5.2. Monitoring és Kiemelt Fejlesztések Osztálya
	2.4.1.6. Nemzetközi Védelmi Ipari Együttműködési Főosztály
	2.4.1.6.1. Multilaterális Együttműködési Osztály
	2.4.1.6.2. Kétoldalú Együttműködési Osztály

4. függelék a 17/2025. (IV. 30.) NGM utasításhoz

1. Az SzMSz 4. függelék II. Gazdasági társaságok című táblázat 9–10. sora helyébe a következő sorok lépnek:

	(A	*B*	*C*	*D*	*E*
1.	*Szervezet megnevezése*	*Jogviszony*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős miniszter, államtitkár*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős helyettes államtitkár*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős szervezeti egység)*
9.	N7 Nemzeti Védelmi Ipari Innovációs Holding Zártkörűen Működő Részvénytársaság	9.1. tulajdonosi jogok gyakorlása	miniszter, közigazgatási államtitkár	tulajdonosi jogok gyakorlásáért felelős helyettes államtitkár	Általános Társasági Portfólió Főosztály
		9.2. szakmai felügyelet	kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár	technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár	Védelmi Ipar Fejlesztési Főosztály
10.	DEBRECEN INTERNATIONAL AIRPORT Korlátolt Felelősségű Társaság	10.1. tulajdonosi jogok gyakorlása	miniszter, közigazgatási államtitkár	tulajdonosi jogok gyakorlásáért felelős helyettes államtitkár	Általános Társasági Portfólió Főosztály
		10.2. szakmai felügyelet	gazdaságfejlesztésért és iparért felelős államtitkár	stratégiai tranzakciókért felelős helyettes államtitkár	Átvilágításokért Felelős Főosztály

2. Az SzMSz 4. függelék II. Gazdasági társaságok című táblázat 17–18. sora helyébe a következő sorok lépnek:

	(A	*B*	*C*	*D*	*E*
1.	*Szervezet megnevezése*	*Jogviszony*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős miniszter, államtitkár*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős helyettes államtitkár*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős szervezeti egység)*
17.	MGFÜ Magyar Gazdaságfejlesztési Ügynökség Közhasznú Nonprofit Korlátolt Felelősségű Társaság	17.1. tulajdonosi jogok gyakorlása	miniszter, közigazgatási államtitkár	tulajdonosi jogok gyakorlásáért felelős helyettes államtitkár	Általános Társasági Portfólió Főosztály
		17.2. szakmai felügyelet	kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár	kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár	Vállalkozásfejlesztési Főosztály
18.	Neumann János Nonprofit Közhasznú Korlátolt Felelősségű Társaság	18.1. tulajdonosi jogok gyakorlása	miniszter, közigazgatási államtitkár	tulajdonosi jogok gyakorlásáért felelős helyettes államtitkár	Általános Társasági Portfólió Főosztály
		18.2. szakmai felügyelet	kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár	technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár	Technológiai Adaptációért és Szabályozásért Felelős Főosztály

3. Az SzMSz 4. függelék II. Gazdasági társaságok című táblázat 23. sora helyébe a következő sor lép:

	(A	*B*	*C*	*D*	*E*
1.	*Szervezet megnevezése*	*Jogviszony*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős miniszter, államtitkár*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős helyettes államtitkár*	*A miniszteri hatáskör gyakorlásával összefüggésben felelős szervezeti egység)*
23.	Magyar Védelmi Exportügynökség Zártkörűen Működő Részvénytársaság	23.1. tulajdonosi jogok gyakorlása	miniszter, közigazgatási államtitkár	tulajdonosi jogok gyakorlásáért felelős helyettes államtitkár	Általános Társasági Portfólió Főosztály
		23.2. szakmai felügyelet	kis- és középvállalkozások fejlesztéséért, technológiáért és védelmi iparért felelős államtitkár	technológiáért, űriparért és védelmi iparért felelős helyettes államtitkár	Védelmi Ipar Fejlesztési Főosztály

A Magyar Államkincstár elnökének 2/2025. (IV. 30.) MÁK utasítása egyes belső szabályozó eszközök hatályon kívül helyezéséről

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontjában meghatározott jogkörömben eljárva a következő utasítást adom ki:

1. § Hatályát veszti

a) a pénzügyi tranzakciós illeték kezelésének eljárásrendjéről szóló 21/2022. (05.06.) számú Elnöki Utasítás,

b) a Magyar Állam nemzetközi pénzügyi és fejlesztési intézetekkel való együttműködésével, tagságával összefüggő kötelezvények kezelésének és a fizetési kötelezettség teljesítésének eljárásrendjéről szóló 11/2023. (03.28.) számú Elnöki Utasítás.

2. § Ez az utasítás a közzétételét követő napon lép hatályba.

Demkó-Szekeres Zsolt s. k.,
elnök

Az Országos Bírósági Hivatal elnökének 2/2025. (IV. 30.) OBH utasítása a bírósági vezetők vezetői tevékenységének vizsgálatáról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés d) pontjában és a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény 137. § (3) bekezdésében kapott felhatalmazás alapján, a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény 76. § (1) bekezdés b) pontjában meghatározott feladatkörömben eljárva, a bírósági vezetők vezetői tevékenysége vizsgálatának részletes szempontjairól és eljárásáról a következő normatív utasítást adom ki:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja

1. § Az utasítás (a továbbiakban: szabályzat) célja, hogy a bírósági szervezet működése hatékonyságának előmozdítása és szervezeti kultúrájának építése érdekében meghatározza a bírósági vezetők igazgatási feladatellátására és személyes kompetenciájára kiterjedő vizsgálat szempontjait, eljárási szabályait, valamint biztosítsa a pártatlan vizsgálat lefolytatásának garanciális követelményeit.

2. A szabályzat hatálya

2. § (1) A szabályzat személyi hatálya az Országos Bírósági Hivatal (a továbbiakban: OBH) elnökének, valamint az ítélőtábla és a törvényszék elnökének kinevezési jogkörébe tartozó bírósági vezetőkre, a vezetői vizsgálatot végző bírókra, valamint a vezetői vizsgálatban közreműködő bírókra és igazságügyi alkalmazottakra terjed ki.

(2) A szabályzat tárgyi hatálya a bírósági vezetők rendes és rendkívüli vezetői vizsgálatára, valamint vezetői utóvizsgálatára terjed ki.

3. A vezetői vizsgálat típusai

3. § A vezetői vizsgálat lehet

a) rendes vezetői vizsgálat,

b) rendkívüli vezetői vizsgálat,

c) vezetői utóvizsgálat.

4. § (1) Rendes vezetői vizsgálat a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény (a továbbiakban: Bszi.) 136. § (1)–(2) bekezdése szerinti vizsgálat.

(2) Rendkívüli vezetői vizsgálat a Bszi. 136. § (3)–(4) bekezdése szerinti vizsgálat.

(3) A vezetői utóvizsgálat a rendes vagy rendkívüli vezetői vizsgálat során feltárt hibák, hiányosságok megszüntetésére tett felszólítás, javaslat, ajánlás végrehajtásának ellenőrzése érdekében elrendelt vizsgálat.

II. FEJEZET
A RENDES VEZETŐI VIZSGÁLAT

4. A vizsgálat tervezése

5. § (1) Az OBH, az ítélőtábla és a törvényszék elnöke (a továbbiakban együtt: a vizsgálat elrendelője) a kinevezési jogkörébe tartozó vezetők rendes vezetői vizsgálatát (jelen fejezet alkalmazásában a továbbiakban: vizsgálat) és a hónap megjelölésével annak várható kezdő időpontját a munkatervben megtervezi.

(2) A tervezéskor figyelemmel kell lenni a vezetői értekezlet ütemezett időpontjára.

5. A vizsgálat elrendelése, elhalasztása

6. § (1) A vizsgálat elrendelője a vizsgálatot írásban rendeli el.

(2) A vizsgálat elrendelője a vizsgálat elrendelésével egyidejűleg értesíti a vizsgálót és a vizsgált vezetőt a vizsgálat elrendeléséről.

(3) A vizsgálatot elrendelő intézkedés tartalmazza

a) a vizsgálat kezdő időpontját,

b) a vizsgálat alapjául szolgáló jogszabály, illetve közjogi szervezetszabályozó eszköz rendelkezéseinek pontos megjelölését,

c) a vizsgált időszakot,

d) a vizsgálat befejezésének időpontját,

e) a vizsgáló nevét, vizsgáló tanács kijelölése esetén a tanács elnökének és tagjainak nevét,

f) szükség esetén a 15. § (2) bekezdése és a 20. § (1) bekezdés a) pontja szerinti döntést,

g) a vizsgálat elrendelője által fontosnak tartott további információkat.

7. § (1) A vizsgálat elrendelője a vizsgálat elrendelését munkaszervezési vagy más fontos okból egy alkalommal legfeljebb hat hónapra elhalaszthatja.

(2) A vizsgálat elrendelője a már elrendelt vizsgálat kezdő időpontját a vizsgált vezető kérelmére méltánylást érdemlő körülmény fennállása esetén legfeljebb hat hónapra, a vizsgálat kezdő időpontjának meghatározásával elhalaszthatja. Méltánylást érdemlő körülmény lehet különösen a vizsgált vezető vagy közeli hozzátartozójának súlyos egészségi állapota.

(3) Halasztás esetén a vizsgálat időpontját a Bszi. 136. § (1) bekezdésében és a szabályzat 5. § (2) bekezdésében foglaltak figyelembevételével kell meghatározni.

6. A vizsgáló kijelölése és összeférhetetlensége

8. § A vizsgálatra három főből álló vizsgáló tanácsot kell kijelölni. A törvényszék székhelye szerinti járásbíróság elnöke és elnökhelyettese kivételével a járásbíróság és a kerületi bíróság (a továbbiakban együtt: járásbíróság) elnökének és elnökhelyettesének, valamint a Bszi. 118. (1) bekezdés c)–f) pontja szerinti vezetőnek a vizsgálatára vizsgáló is kijelölhető. A továbbiakban a vizsgálóra vonatkozó rendelkezéseket a vizsgáló tanácsra és annak tagjaira is alkalmazni kell.

9. § (1) A vizsgálót a vizsgálat elrendelője jelöli ki.

(2) Nem jelölhető ki vizsgálónak

a) az, aki nem rendelkezik legalább 3 éves tényleges vezetői gyakorlattal,

b) az, akinek a rendes vezetői vizsgálatában a vizsgált vezető vizsgálóként közreműködött.

(3) A vizsgálat elrendelője vizsgálónak, vizsgáló tanács eljárása esetén a tanács elnökének a kinevezési jogkörébe tartozó, a vizsgált vezetővel legalább azonos beosztású, azonos beosztás esetén nála hosszabb vezetői gyakorlattal rendelkező bírósági vezetőt jelöl ki.

(4) Ha nincs a (3) bekezdés szerint kijelölhető vizsgáló, akkor a vizsgálat elrendelője az OBH elnökének kinevezési jogkörébe tartozó vezetőt jelöl ki vizsgálónak.

(5) Az OBH elnöke – a (2)–(3) bekezdéstől eltérően – vizsgálónak az OBH-ba határozatlan időre beosztott bírót is kijelölhet.

10. § (1) Nem jelölhető ki vizsgálónak

a) az OBH elnökének, elnökhelyettesének,

b) a vizsgált bírósági vezető tekintetében kinevezési jogkört gyakorló ítélőtábla vagy törvényszéki elnöknek,

c) a vizsgált bírósági vezető szolgálati helye szerinti ítélőtábla vagy törvényszék elnökhelyettesének, kollégiumvezetőjének, kollégiumvezető-helyettesének,

d) a vizsgált bírósági vezető szolgálati helye szerinti járásbíróság elnökének, elnökhelyettesének,

e) a vizsgált bírósági vezetőnek

a bírák jogállásáról és javadalmazásáról szóló 2011. évi CLXII. törvény (a továbbiakban: Bjt.) 71/A. § (1) bekezdése szerinti hozzátartozója.

(2) Nem jelölhető ki vizsgálónak, akitől a vizsgálat tárgyilagos lefolytatása nem várható el.

11. § (1) A vizsgálat elrendelője az összeférhetetlenség fennállását a vizsgálat alatt folyamatosan vizsgálja.
(2) A vizsgáló köteles haladéktalanul írásban bejelenteni, ha vele szemben összeférhetetlenségi ok merül fel.
(3) Összeférhetetlenségi okot a vizsgált vezető is bejelenthet. A vizsgált vezető az összeférhetetlenségi okot köteles a tudomásszerzést követően haladéktalanul bejelenteni.
(4) A vizsgálat elrendelője a bejelentést 3 munkanapon belül elbírálja. Amennyiben a vizsgálat elrendelője a bejelentésnek helyt ad, vagy saját maga észlel összeférhetetlenséget, másik vizsgálót jelöl ki.
(5) Nem lehet elutasítani a vizsgálónak azt a bejelentését, mely szerint tőle a vizsgálat tárgyilagos lefolytatása nem várható el.

7. A vizsgálatban részt vevők jogai és kötelezettségei

12. § A vizsgáló tanács elnöke vezeti és koordinálja a vizsgáló tanács tevékenységét.

13. § (1) A vizsgáló a tevékenysége során
a) a vizsgálattal kapcsolatos iratokba, dokumentumokba, nyilvántartásokba, adatbázisokba – törvényi korlátozások figyelembevételével – betekinthet,
b) a vizsgálattal kapcsolatos iratokról – törvény kizáró rendelkezése hiányában – másolatot, kivonatot készíthet,
c) a vizsgált vezető által használt épületekbe, helyiségekbe beléphet,
d) a vizsgálat elrendelőjétől, a vizsgált vezető szolgálati helye szerinti bíróság elnökétől nyilatkozatot, adatszolgáltatást vagy okirat bemutatását kérheti.
(2) A vizsgáló a tevékenysége során befolyástól és elfogultságtól mentesen jár el.
(3) A vizsgáló részére a vizsgálat időtartamára a törvényszék, illetve az ítélőtábla elnöke hozzáférést biztosít a vizsgált vezető által irányított vagy igazgatott szervezeti egység elektronikus nyilvántartásaihoz és adatbázisaihoz.
(4) A vizsgált vezető szolgálati helye szerinti bíróság elnöke köteles
a) biztosítani a vizsgálat végrehajtásához szükséges feltételeket,
b) megadni a vizsgáló számára a szükséges tájékoztatásokat,
c) elősegíteni a vizsgáló és a vizsgált vezető együttműködését.
(5) Az (1) bekezdés d) pontjában foglalt személy köteles a vizsgálónak a szükséges tájékoztatást, nyilatkozatot és adatszolgáltatást megadni, valamint a kért okiratot bemutatni.
(6) Az (1) bekezdés d) pontjában felsorolt személy, valamint a vizsgáló a vizsgálat során együttműködni kötelesek.

8. A vizsgálat módszerei

14. § A vizsgálat módszerei:
a) iratvizsgálat,
b) elektronikus információs rendszer adatainak vizsgálata,
c) személyes megbeszélés,
d) részvétel a vizsgált vezető által tartott értekezleten,
e) interjú,
f) kérdőív,
g) helyszíni bejárás.

15. § (1) A 21. § szerinti kapcsolatfelvételt követően a vizsgált vezető a vizsgáló részére haladéktalanul megküldi
a) a vezetői pályaművét,
b) amennyiben beszámoló készítésére kötelezett, a vizsgált időszakban készült éves beszámolóit,
c) a magas színvonalú és időszerű ítélkezés érdekében hozott vezetői intézkedést tartalmazó két, általa választott iratot,
d) egy releváns probléma megoldására szolgáló iratot.
(2) A vizsgálat elrendelője a vizsgálatot elrendelő intézkedésében az (1) bekezdésben meghatározottakon túl további iratok megküldését is előírhatja.
(3) A vizsgáló további iratok bemutatását is kérheti, és betekinthet az elektronikus informatikai rendszer adataiba.

16. § (1) A vizsgáló személyes megbeszélést folytat a vizsgált vezetővel a vizsgálat tárgyát képező témakörökről.
(2) A személyes megbeszélés során a vizsgált vezető is javasolhat a vezetői tevékenységét érintő témákat.
(3) A személyes megbeszélésen elhangzottakról a vizsgáló feljegyzést készít.

17. § (1) A vizsgáló bírósági elnök vizsgálata esetén vezetői értekezleten, kollégiumvezető vizsgálata esetén kollégiumi ülésen, csoportvezető vizsgálata esetén csoportértekezleten vesz részt, ahol meggyőződik a vizsgált vezető kommunikációs, lényeglátási és problémakezelési képességéről.
(2) Az értekezleten tapasztaltakról a vizsgáló feljegyzés készít.
(3) Amennyiben a vizsgálat ideje alatt a vizsgált vezető nem tart értekezletet, illetve ülést, a vizsgáló bekéri a legutóbbi értekezlet, illetve ülés jegyzőkönyvét, emlékeztetőjét.

18. § A vizsgáló interjút készít
a) ítélőtáblai, törvényszéki elnök vizsgálata esetén a bírói tanács elnökével, a gazdasági hivatal vezetőjével, valamint az ítélőtábla vagy a törvényszék kollégiumvezetőivel;
b) ítélőtáblai és törvényszéki elnökhelyettes vizsgálata esetén az ítélőtábla vagy a törvényszék elnökével, valamint az ítélőtábla vagy a törvényszék kollégiumvezetőivel;
c) kollégiumvezető vizsgálata esetén az ítélőtábla vagy a törvényszék elnökével, valamint amennyiben van, akkor a kollégiumvezető-helyettessel;
d) járásbírósági elnök vizsgálata esetén a törvényszék kollégiumvezetőivel;
e) járásbírósági elnökhelyettes, kollégiumvezető-helyettes, csoportvezető, csoportvezető-helyettes vizsgálata esetén a vizsgált vezető közvetlen felettes vezetőjével.

19. § A törvényszéki és ítélőtáblai elnök vizsgálata esetén a vizsgáló tanács elnöke az OBH főosztályvezetőit felkéri az 1. melléklet szerinti kérdőív kitöltésére.

20. § (1) A vizsgáló helyszíni bejárást végez, ha azt
a) a vizsgálat elrendelője a vizsgálatot elrendelő intézkedésében előírja,
b) a vizsgálat szempontjából lényegesnek ítélt körülmény megállapításához szükségesnek tartja,
c) a vizsgált vezető kéri.
(2) A vizsgáló a helyszíni bejárás során megvizsgálja
a) a vizsgált vezető közvetlen munkakörnyezetét,
b) az épületek állapotát,
c) az irodák, a tárgyalótermek és egyéb helyiségek állapotát,
d) az ügyfélforgalom előtt nyitva álló helyiségek állapotát és megközelíthetőségét,
e) az eligazodást segítő információs és tájékoztató táblákat, feliratokat,
f) a munkatársak irodai elhelyezését, az irodák felszereltségét, állapotát,
g) az informatikai eszközökkel való felszereltséget.

9. A vizsgálat szempontjai és lefolytatása

21. § (1) A vizsgáló a 6. § (3) bekezdés a) pontjában meghatározott időpont elteltét követően haladéktalanul írásban vagy elektronikus úton felveszi a kapcsolatot a vizsgált vezetővel, és intézkedik a vizsgálathoz szükséges iratok beszerzése, valamint az elektronikus információs rendszerekhez való hozzáférések engedélyezése iránt.
(2) A vizsgáló a kapcsolat felvételekor tájékoztatja a vizsgált vezetőt a vizsgálat menetéről, módszereiről, és egyezteti vele a személyes megbeszélés, továbbá a vezetői értekezleten való részvétel időpontját.

22. § (1) A vizsgálat során a vizsgáló megvizsgálja
a) a jogszabályban, az OBH elnökének utasításában, határozatában, a bíróság szervezeti és működési szabályzatában, valamint a kinevezési jogkör gyakorlójának és felettes vezetőjének intézkedésében meghatározott feladatok végrehajtását;
b) a pályaműben szereplő tervek megvalósítását, az abban kitűzött célok és intézkedések végrehajtását;
c) a vezetői kompetenciák körében
ca) a kommunikációs, kapcsolattartási és konfliktuskezelési képességet,
cb) a stratégiai gondolkodás képességét,

cc) a változáskezelési, szervezetirányítási képességet és tevékenységet,

cd) a saját motiváltság jellemzőit és a munkatársak motiválásának képességét.

(2) Bírósági elnök vizsgálata esetén az (1) bekezdésben foglaltak mellett a vizsgáló megvizsgálja

a) a magas színvonalú és időszerű ítélkezés érdekében tett intézkedéseket, azok eredményességét az ítélkezés minőségi mutatói és időszerűsége alapján;

b) az ítélkezés személyi feltételeinek biztosítása körében

ba) az optimális létszámgazdálkodás és arányos munkateher kialakítása érdekében tett intézkedéseket,

bb) az egyenlő bánásmód elvének érvényesülését különösen az előmenetel, az illetményen kívüli juttatások és az egyéb, dolgozóknak biztosított kedvezmények tekintetében,

bc) a foglalkoztatásra vonatkozó szabályok alkalmazásának, a munkáltatói jogkörök gyakorlásának jogszerűségét, a méltányossági döntési jogkör gyakorlását, a nyilvántartások vezetését;

c) az ítélkezés tárgyi feltételeinek biztosítása körében

ca) az észszerű és költséghatékony gazdálkodás megvalósulását,

cb) a létesítmény- és eszközgazdálkodás körében tett intézkedéseket,

cc) a munkakörülmények javítása érdekében tett intézkedéseket,

cd) az informatikai biztonság érdekében tett intézkedéseket.

(3) Elnökhelyettes vizsgálata esetén az (1) bekezdésben foglaltak mellett a vizsgáló a (2) bekezdésben foglaltakat is megvizsgálja, ha a vizsgált időszakban a bíróság elnökét annak akadályoztatása miatt – ideértve azt az esetet is, ha a tisztség nem volt betöltve – helyettesítette.

(4) A kollégiumvezető és a kollégiumvezető-helyettes vizsgálata esetén az (1) bekezdésben foglaltak mellett a vizsgáló megvizsgálja a kollégium munkájának szervezését és e körben a magas színvonalú és időszerű ítélkezés érdekében tett intézkedéseket, azok eredményességét az ítélkezés minőségi mutatói és időszerűsége alapján.

(5) A csoportvezető és a csoportvezető-helyettes vizsgálata esetén az (1) bekezdésben foglaltak mellett a vizsgáló megvizsgálja a csoport munkájának szervezését.

23. § A vizsgáló a tevékenysége során a vizsgálati szempontok teljes körű és a 14. § szerinti vizsgálati módszerekkel alátámasztott kielemzésére törekszik.

24. § (1) A vizsgáló a vizsgálat kezdő időpontjától számított 45 napon belül a vizsgálat tapasztalatairól vizsgálati jelentést és értékelési javaslatot készít. A vizsgálati jelentés határidőben történő elkészítéséért és annak tartalmáért a vizsgáló felelős.

(2) Vizsgáló tanács eljárása esetén a tanács tagjai a vizsgálat tapasztalatait megvitatják, és megállapításaikat részjelentésekben rögzítik. A vizsgálati jelentést és az értékelési javaslatot a vizsgáló tanács elnöke készíti el.

(3) A vizsgálati jelentés tartalmazza a vizsgálat során tapasztalt tényeket, körülményeket, rögzíti az ezeket megalapozó iratokat, a vizsgáló megállapításait. A jelentésben ki kell térni arra, hogy a vizsgált vezető a vezetői feladatait mennyiben teljesíti, ezek ellátásához szükséges kompetenciákkal rendelkezik-e, vezetői munkájának melyek az erősségei és a fejlesztendő területei. A vizsgáló a vizsgálati jelentésben a feltárt hibák, hiányosságok megszüntetésére intézkedési javaslatot tehet.

(4) A vizsgáló a vizsgálatot elrendelő és a vizsgált vezető részére megküldi a vizsgálati jelentést, az értékelési javaslatot és a vizsgálat során keletkezett valamennyi iratot.

(5) A vizsgálati jelentést alátámasztó egyéb iratot a vizsgált vezető vagy a vizsgálat elrendelőjének kérésére kell megküldeni.

(6) A vizsgált vezető a vizsgálati jelentésre és az értékelési javaslatra annak kézhezvételét követő 8 napon belül a vizsgálónál és a vizsgálat elrendelőjénél írásban észrevételt tehet.

25. § (1) A vizsgálat elrendelője kitűzi a szóbeli értékelés időpontját, amelyről a vizsgált vezetőt, valamint a vizsgálót és amennyiben a vizsgált vezető felettes vezetője nem azonos a vizsgálat elrendelőjével, akkor a felettes vezetőjét írásban értesíti.

(2) A szóbeli értékelésen a vizsgálat elrendelője, az (1) bekezdés szerint értesített személy és a jegyzőkönyvvezető lehet jelen. A szóbeli értékelésről jegyzőkönyv készül.

(3) A vizsgálat elrendelője a szóbeli értékelésen megállapítja a vizsgálat eredményét.

(4) Az értékelés eredményeként a vizsgált vezető alkalmas vagy nem alkalmas értékelést kaphat.

(5) A vizsgálatot elrendelő az értékelésben a vizsgált vezetőt határidő tűzésével felszólíthatja a feltárt hibák, hiányosságok megszüntetésére, részére javaslatot, ajánlást tehet.

(6) A vizsgálatot elrendelő az írásba foglalt értékelést és a jegyzőkönyvet a szóbeli értékelést követő 5 munkanapon belül megküldi a vizsgált vezetőnek.

26. § Az értékeléssel szemben a Bjt. 80. §-a és 85. § (4) bekezdése, valamint a Bszi. 140. §-a szerint van helye jogorvoslatnak.

10. A tanácselnök vizsgálata

27. § (1) A II. Fejezet rendelkezéseit nem kell alkalmazni a tanácselnök vizsgálatára.
(2) A tanácselnök vezetői tevékenységét lehetőleg a rendszeres bírói értékelés alkalmával kell megvizsgálni.

III. FEJEZET
A RENDKÍVÜLI VEZETŐI VIZSGÁLAT

28. § (1) A vizsgálatot elrendelő intézkedésben a 6. § (3) bekezdésében foglaltak mellett meg kell határozni a vizsgálatra okot adó körülményeket és a vizsgálat szempontjait.
(2) A Bszi. 136. § (4) bekezdés b) pontjában meghatározott esetben a vizsgálat elrendelője a felmentés kezdeményezésének kézhezvételétől számított 30 napon belül elrendeli a vizsgálatot.
(3) A vizsgáló a 14. §-ban meghatározott vizsgálati módszereket szabadon megválaszthatja és alkalmazhatja.
(4) A vizsgáló az eljárása során kizárólag a 28. § (1) bekezdésében meghatározott szempontokat vizsgálhatja.
(5) A rendkívüli vezetői vizsgálatra – az 5. §, a 7. §, a 9. § (2) bekezdés b) pontja, a 15–20. §, a 22. § és a 27. § kivételével – egyebekben a II. Fejezet rendelkezéseit is alkalmazni kell.

IV. FEJEZET
A VEZETŐI UTÓVIZSGÁLAT

29. § (1) Ha a vizsgálat elrendelője az értékelésben határidő tűzésével a feltárt hibák, hiányosságok megszüntetésére szólította fel a vizsgált vezetőt, a határidő elteltét követő 30 napon belül a végrehajtás ellenőrzésére vizsgálatot rendel el.
(2) A vezetői utóvizsgálatra egyebekben a 28. § (1) és (3)–(5) bekezdése rendelkezéseit kell alkalmazni.

V. FEJEZET
ZÁRÓ RENDELKEZÉSEK

11. Hatályba léptető rendelkezések

30. § Ez az utasítás 2025. június 15. napján lép hatályba, rendelkezéseit a hatálybalépését követően elrendelt vezetői vizsgálatokra kell alkalmazni.

12. Módosító és hatályon kívül helyező rendelkezések

31. § (1) A bíróságok igazgatásáról rendelkező szabályzatról szóló 6/2015. (XI. 30.) OBH utasítás (a továbbiakban: igazgatási szabályzat) 47. § (3) és (4) bekezdése helyébe a következő rendelkezések lépnek:
„(3) Az OBH elnöke elrendelhet az igazgatási vizsgálat körében különösen rendes, rendkívüli, eseti, cél- és hatásvizsgálatot, melyeket helyszíni vizsgálat keretében vagy külső vizsgáló kijelölésével is foganatosíthat.
(4) Az OBH elnöke az ítélőtábla és a törvényszék elnökét évente írásban beszámoltatja.”
(2) Az igazgatási szabályzat 74. és 75. §-a helyébe a következő rendelkezések lépnek:
„74. § (1) Az igazgatási vizsgálat elrendelésének célja:
a) az adott bírósági szervezet vagy szervezeti egység működési rendjének, szervezeti és gazdálkodási rendszerének átvilágítása és fejlesztése;
b) az adott bírósági szervezet, szervezeti egység törvényes és szabályszerű működésének ellenőrzése;

c) az adott bírósági szervezetben vagy szervezeti egységben végzett egyes feladatkörök ellátásával kapcsolatos gyakorlat átvilágítása és fejlesztése a szükséges és indokolt igazgatási intézkedések megtétele érdekében azért, hogy javuljon az érintett szervezet vagy szervezeti egység működésének hatékonysága, szakmai színvonala, a vezetői tevékenység és a feladatellátás minősége;

d) a hibák és a hiányosságok feltárása.

(2) Az igazgatási vizsgálat lehet különösen rendszeres, rendkívüli, cél- és utóvizsgálat, melyeket helyszíni vizsgálat keretében vagy külső vizsgáló bevonásával is foganatosíthat az elrendelő. Az igazgatási vizsgálatot elrendelő bíróság elnöke a fentieken kívül egyéb igazgatási vizsgálat elrendelésére is jogosult.

75. § (1) Az igazgatási vizsgálatot

a) az OBH elnöke határozattal az ítélőtáblára, a törvényszékre,

b) az ítélőtábla és a törvényszék elnöke intézkedésével a vezetése vagy felügyelete alá tartozó bíróságra, kollégiumra vagy bírósági szervezeti egységre,

c) a járásbíróság elnöke intézkedésével a vezetése alatt álló bíróságra vagy a bíróság szervezeti egységére

rendeli el.

(2) Az igazgatási vizsgálat elrendeléséről szóló határozatnak vagy intézkedésnek tartalmaznia kell különösen:

a) a lefolytatandó vizsgálat alapját, indokát, típusát, annak jellegét az alapul szolgáló jogszabályhely – ideértve a jelen szabályzatra történő hivatkozást is – megjelölésével,

b) a vizsgálat célját, a vizsgálat terjedelmét – ezen belül a vizsgált időszakot és folyamatot – esetlegesen a megvalósításhoz ajánlott vizsgálati módszereket és a vizsgálat tárgyát,

c) a vizsgálatot végző személy vagy személyek (vizsgáló team) – ez utóbbi esetben a csoport vezetőjének – kijelölését,

d) a vizsgálat kezdő és befejező időpontját, valamint a vizsgálati jelentés elkészítésének határidejét.

(3) Az igazgatási vizsgálatok elrendelése során törekedni kell arra, hogy a vizsgálat elrendelésével elérni kívánt cél és a vizsgálat elvégzésével járó teher arányos legyen."

(3) Az igazgatási szabályzat a következő 76/A–76/D. §-sal egészül ki:

„76/A. § (1) Az OBH elnöke által elrendelt vizsgálatot az OBH illetékes főosztálya vagy az OBH elnöke által kijelölt személy vagy személyek (vizsgáló team), a bíróság elnöke által elrendelt vizsgálatot a bíróság elnöke vagy általa kijelölt más bírósági vezető(k), bíró(k) vagy igazságügyi alkalmazott(ak) folytatják le.

(2) Az igazgatási vizsgálatot elvégezheti az elrendelő által kijelölt, de a munkáltatói jogkörébe nem tartozó külső vizsgáló is, amennyiben a vizsgálat tárgya, terjedelme, ideje és a speciális szaktudás azt indokolttá teszi.

(3) Külső vizsgálóként kijelölhető az ellenőrzéssel nem érintett bírósági szervezet vagy szervezeti egység

a) elnöke és elnökhelyettese,

b) kollégiumvezetője és kollégiumvezető-helyettese,

c) csoportvezetője és csoportvezető-helyettese,

d) tanácselnöke,

e) bírája,

f) igazságügyi alkalmazottja.

76/B. § (1) A vizsgálatot úgy kell megtervezni és lefolytatni, hogy az biztosítsa a magas színvonalú ellenőrzés gazdaságos, hatékony, eredményes és megfelelő időben történő elvégzését, továbbá az átláthatóságot.

(2) A vizsgálatot végző személynek a tevékenysége során joga van

a) a vizsgálat jellegéhez igazodóan a belső határozatokba, elnöki intézkedésekbe, utasításokba, igazgatási iratokba és nyilvántartásokba betekinteni,

b) a bíróság elnökétől vagy más bírósági vezetőtől, bírótól vagy igazságügyi alkalmazottól a vizsgálat céljához kapcsolódóan szóbeli vagy írásbeli nyilatkozatot, jelentést, adatszolgáltatást vagy okiratot kérni,

c) a szükséges iratokról, dokumentumokról másolatot vagy kivonatot készíteni vagy készíttetni.

(3) A vizsgálattal érintett bíróság vagy szervezeti egység vezetője köteles

a) biztosítani a vizsgálat lefolytatásához szükséges feltételeket,

b) megadni a vizsgáló számára a szükséges tájékoztatásokat és az általa kért adatokat,

c) a vizsgálatot végzővel együttműködni.

(4) A bíróság elnöke vagy a kijelölt vizsgáló a kiadott intézkedések és feladatok végrehajtását a helyszínen közvetlenül is megvizsgálhatja, ellenőrizheti.

76/C. § (1) A vizsgáló(k) a vizsgálat elrendeléséről szóló iratban megjelölt határidőn belül köteles(ek) elkészíteni a részletes vizsgálati jelentést, amely az ellenőrzés során tapasztalt tényeket, körülményeket tartalmazza, rögzíti az előbbieket megalapozó dokumentumokat, a vizsgáló(k) megállapításait és az esetleges intézkedési javaslatokat.

(2) Ha a vizsgálatot többen végezték, a vizsgálók a megállapításaikat részjelentésekben rögzítik, melyek összegzéseként állítja össze a vizsgálat vezetője az összefoglaló jelentést.

(3) A jelentéshez a megállapításokat alátámasztó függelékeket, mellékleteket és táblázatokat is csatolni kell.

76/D. § (1) A vizsgálattal érintett bírósági vezetőnek lehetőséget kell biztosítani, hogy a vizsgálati jelentés megállapításaira észszerű határidőn belül észrevételeket tehessen.

(2) Az igazgatási vizsgálatot a Bszi. 137. § (1) bekezdése szerinti hatvan napon belüli határidőn belül be kell fejezni, mely határidőbe az (1) bekezdés szerinti észrevétel előterjesztésére megszabott határidő is beleszámít.

(3) A vizsgálat elrendelője a vizsgálat megállapításaitól függően teszi meg a hatáskörébe tartozó igazgatási intézkedéseket.

(4) A vizsgálat eredményét a vizsgálati jelentés elkészítésétől számított tizenöt napon belül ismertetni kell a vizsgálattal érintett bíróság vezetőjével és az érintett szervezeti egységbe beosztott bírákkal és igazságügyi alkalmazottakkal."

(4) Az igazgatási szabályzat a következő 2.4.4.3.2.4. alcímmel egészül ki:

„2.4.4.3.2.4. Az utóvizsgálat

80/A. § Az utóvizsgálat az intézkedések nyomon követése érdekében elrendelt vizsgálat, amelynek a célja a vizsgálati jelentésben rögzített és az elrendelő által meghozott intézkedések végrehajtásáról, ennek keretében arról a tényről történő bizonyosságszerzés, hogy az érintett bíróság vagy az érintett szervezeti egység és annak vezetője megfelelően végrehajtja-e az intézkedéseket."

(5) Az igazgatási szabályzat a következő 205/A. §-sal egészül ki:

„205/A. § Ezen utasításnak a bírósági vezetők vezetői tevékenységének vizsgálatáról szóló 2/2025. (IV. 30.) OBH utasítás (a továbbiakban: Mód.1.) 31. § (2) bekezdésével megállapított 75. § (1) bekezdés a) pontját és 75. § (2) bekezdését a Mód.1. hatálybalépését követően elrendelt vizsgálatokra kell alkalmazni."

(6) Az igazgatási szabályzat

1. 47. § (7) bekezdésében a „soros vagy soron kívüli" szövegrész helyébe a „rendes vagy rendkívüli" szöveg,
2. 2.4.4.3.2.1. alcím címében a „rendszeres" szövegrész helyébe a „rendes" szöveg

lép.

(7) Hatályát veszti az igazgatási szabályzat

a) 47. § (1) bekezdésében az „és az általa meghozott igazgatási szabályozók végrehajtását" szövegrész,
b) 47. § (5) és (6) bekezdése,
c) 50. § (2) bekezdése,
d) 2.4.4.1. és 2.4.4.2. alcíme,
e) 77. § (2) bekezdése,
f) 78. §-a.

32. § (1) A bíró munkájának értékelési rendjéről és a vizsgálat részletes szempontjairól szóló szabályzatról szóló 8/2015. (XII. 12.) OBH utasítás (a továbbiakban: bíróvizsgálati szabályzat) 31. §-a a következő (5) bekezdéssel egészül ki:

„(5) A tanácselnök vizsgálatakor a vezetői tevékenységet is vizsgálni kell."

(2) A bíróvizsgálati szabályzat 40. §-a a következő (6) bekezdéssel egészül ki:

„(6) Ezen utasításnak a bírósági vezetők vezetői tevékenységének vizsgálatáról szóló 2/2025. (IV. 30.) OBH utasítás (a továbbiakban: Módut.2.) 32. § (1) bekezdésével megállapított 31. § (5) bekezdését a Módut.2. hatálybalépését követően elrendelt vizsgálatokra kell alkalmazni."

Dr. Senyei György s. k.,
az Országos Bírósági Hivatal elnöke

1. melléklet a 2/2025. (IV. 30.) OBH utasításhoz

…… szám

Írásbeli kérdőív a törvényszéki és ítélőtáblai elnökök vezetői vizsgálatához

OBH … Főosztály
részére
Budapest

Tisztelt Főosztályvezető Asszony/Úr!

Az OBH elnöke …… számú intézkedésével elrendelte …… törvényszéki/ítélőtáblai elnök vezetői tevékenységének rendes vizsgálatát. Ennek alapján kérem, hogy 8 napon belül szíveskedjék az alábbi kérdésekre válaszolni.

1) A vizsgált vezető a jogszabályokban, az OBH elnöki szabályzatokban, eseti megkeresésekben írt jelentéstételi, tájékoztatási kötelezettségét határidőben teljesíti-e?
2) Milyen minőségűek a vizsgált vezető jelentései, tájékoztatásai?
3) Milyennek tartja a vizsgált vezető együttműködését, kommunikációját az Ön által vezetett főosztállyal?
4) Egyéb, a főosztályvezető által fontosnak tartott megállapítás.

(Dátum)

(Aláírás)

Az országos rendőrfőkapitány 12/2025. (IV. 30.) ORFK utasítása az Információbiztonsági Szabályzatról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontjában, valamint a Rendőrségről szóló 1994. évi XXXIV. törvény 6. § (1) bekezdés b) pontjában foglaltak alapján, a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 6. § (3) bekezdés 7. pontjában meghatározott feladat végrehajtása érdekében kiadom az alábbi utasítást:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. Az utasítás hatálya

1. Az utasítás hatálya kiterjed
   a) az Országos Rendőr-főkapitányságra (a továbbiakban: ORFK);
   b) a Készenléti Rendőrségre, a Repülőtéri Rendőr Igazgatóságra, a Nemzetközi Bűnügyi Együttműködési Központra, a Rendőrségi Oktatási és Kiképző Központra, a Nemzetközi Oktatási Központra és a vármegyei (fővárosi) rendőr-főkapitányságokra (a továbbiakban együtt: területi szerv);
   c) a rendőrkapitányságokra és a határrendészeti kirendeltségekre (a továbbiakban együtt: helyi szerv).
2. Az utasítás tárgyi hatálya a minősített adatokat kezelő rendszerek kivételével kiterjed az általános rendőrségi feladatok ellátására létrehozott szerv (a továbbiakban: Rendőrség) által működtetett, üzemeltetett vagy használt valamennyi, a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben (a továbbiakban: Kiberbiztonsági törvény) meghatározott elektronikus információs rendszerre (a továbbiakban: EIR) és azok környezetét alkotó rendszerelemre (a működéshez szükséges infrastruktúra, fizikai környezet, hardver, kommunikáció és hálózat, szoftver, folyamat), az informatikai folyamatban szereplő valamennyi dokumentációra, azok teljes életciklusában.

2. Értelmező rendelkezések

3. Az utasítás alkalmazásában
   3.1. *adatátvitel:* az adatok EIR-ek, rendszerelemek közötti továbbítása;
   3.2. *adathordozó:* az EIR-hez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása megvalósítható, valamint a digitális adatok tárolására és feldolgozására alkalmas mobil eszköz;
   3.3. *adminisztrátori dokumentáció:* az EIR és annak környezetét alkotó rendszerelem biztonságos konfigurálását, telepítését és üzemeltetését, a biztonsági funkciók hatékony alkalmazását és fenntartását, a konfigurációval és az adminisztratív funkciók használatával kapcsolatos ismert sérülékenységeket tartalmazó dokumentáció;
   3.4. *alkalmazás:* egy célfeladatot megvalósító szoftver;
   3.5. *EIR üzemeltető:* az a szervezeti egység vagy elem, amely biztosítja az EIR üzemszerű működését;
   3.6. *felelős szakterület:* az a szervezeti egység vagy elem, amely az EIR által kezelt adatok adatkezeléséért felelős, valamint az EIR környezetét alkotó rendszerelem esetén annak üzemeltetője;
   3.7. *felhasználó:* az a személy, aki egy EIR vagy annak környezetét alkotó rendszerelem használója;
   3.8. *hardver:* informatikai eszközök kézzel megfogható részeinek gyűjtőneve;
   3.9. *hálózat:* az informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége;
   3.10. *hálózati aktív eszközök:* a hálózat működését biztosító elektronikus elemek (különösen a tűzfal, a router, a switch, a hub, az optikai átkapcsoló);
   3.11. *hálózati passzív eszközök:* a hálózati aktív eszközök kapcsolatát és kommunikációját biztosító elemek (különösen a kábelezés, a kábelcsatornák, a fali csatlakozók és a rendezőszekrények);
   3.12. *hozzáférés:* az EIR-ben vagy annak környezetét alkotó rendszerelemben tárolt adatok, információk elérésének lehetősége a felhasználó vagy egy másik EIR és annak környezetét alkotó rendszerelem által;
   3.13. *informatikai biztonság:* az EIR olyan állapota, amelyben a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított, valamint a rendszerelemek biztonsága zárt, teljes körű, folytonos és a kockázatokkal arányos;

3.14. *informatikai erőforrásokat koncentráltan tartalmazó helyiségek:* olyan, speciálisan kialakított, védett területek, ahol az EIR környezetét alkotó rendszerelem kritikus részei, különösen a szerverek, a hálózati eszközök, az adattárolók és egyéb számítástechnikai berendezések találhatók;

3.15. *informatikai eszköz:* minden olyan digitális eszköz és ennek funkcionális tartozéka, amely adatok összegyűjtésére, feldolgozására (különösen rendezésére, csoportosítására, kiszámítására), előállítására, tárolására és megjelenítésére, illetve az e tevékenységekkel kapcsolatos adatmódosításra és adattovábbításra alkalmas (így különösen a hardver, a szoftver, a hálózati eszközök és a perifériák);

3.16. *informatikai rendszerüzemeltető:* az a szervezeti egység vagy elem, amely biztosítja az EIR környezetét alkotó rendszerelemek üzemszerű működését;

3.17. *információbiztonság:* olyan előírások, szabályok és szabványok betartásának eredménye, amelyek az EIR-ben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az EIR és elemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítását érintik;

3.18. *információbiztonságért felelős személy:* az EIR biztonságáért felelős személy;

3.19. *információbiztonság-tudatosság:* olyan gondolkodás és magatartásforma, amely biztosítja, hogy a szervezet alkalmazottai elismerik, elfogadják és alkalmazzák a szervezetük információbiztonsági adminisztratív, logikai és fizikai védelmi intézkedéseit;

3.20. *integritás:* a sérthetetlenségen túl a teljességet, továbbá az ellentmondás-mentességet jelenti, amelynek eredményeként az információ valamennyi része konzisztensen rendelkezésre áll, elérhető;

3.21. *intézkedés:* adminisztratív, műszaki, irányítási vagy jogi természetű kockázatkezelési eszköz, beleértve a szabályzatokat, az eljárásokat, az irányelveket, a gyakorlatokat és a képzést;

3.22. *intézkedési terv:* az EIR biztonsági osztályának megfelelő követelmények teljesítéséhez szükséges korrekciós intézkedések, valamint az információbiztonság és az ellátási lánc kockázatkezelése alapján fennmaradó kockázatok kezelésének terve;

3.23. *javítás:* előre nem tervezett hibaelhárítási feladat, amely indokolt esetben az EIR és annak környezetét alkotó rendszerelem konfigurációjának változásával jár;

3.24. *jogosultság:* jog, amely meghatározza, hogy a felhasználó vagy az EIR és annak környezetét alkotó rendszerelem az elérhető adatokon és információkon milyen műveletet végezhet; jogosultságot csak hozzáféréssel rendelkező személyek kaphatnak;

3.25. *karbantartás:* tervezetten végzett munka, amely indokolt esetben az EIR és annak környezetét alkotó rendszerelem konfigurációjának változásával jár, karbantartásnak minősül különösen a biztonsági réseket befoltozó hibajavítások telepítése;

3.26. *kártékony kód:* rosszindulatú számítógépes programok összefoglaló neve, különösen a vírus, a féreg, a kémprogram, a zsarolóprogram és az informatikai rendszerben láthatatlanul megbúvó, egy támadónak hozzáférést és jogosultságot biztosító eszköz;

3.27. *kibertér:* a számítógépes hálózatok és az általuk összekötött számítógépek és egyéb berendezések által alkotott virtuális tér, az a környezet, amelyben az adat technikai eszközökön (számítógépes hálózatokon) keresztül áramlik, elektronikus adatok tárolódnak, online adatforgalom és kommunikáció zajlik;

3.28. *korrektív kontroll:* az eredeti állapot visszaállítását célzó intézkedés;

3.29. *maximális időablak:* az üzletmenet során igénybe vett informatikai szolgáltatások kimaradásának jogszabály vagy kockázatelemzés alapján az 1. pont a) és b) alpontjában meghatározott szerv vezetője által meghatározott leghosszabb időtartama;

3.30. *menedzselés:* az informatikai rendszerek és folyamatok olyan irányítása és felügyelete, amely biztosítja a biztonsági célok elérését, a kockázatok folyamatos felmérését, a szükséges ellenőrzéseket és beavatkozásokat, valamint a rendszeres frissítést és fejlesztést a fenyegetések hatékony kezelése érdekében;

3.31. *privilegizált felhasználó:* az a felhasználó, aki az EIR és annak környezetét alkotó rendszerelem, rendszer, hálózat üzemeltetési vagy fejlesztési feladatainak végrehajtásához emelt szintű jogosultsággal rendelkezik;

3.32. *szerver:* olyan számítógép vagy szoftver, amely más számítógépek számára a rajta tárolt vagy előállított adatok felhasználását, a szerver hardver-erőforrásainak (különösen a nyomtató, a háttértárolók és a processzor) kihasználását, illetve más szolgáltatások elérését teszi lehetővé;

3.33. *szoftver:* elektronikus adatfeldolgozó berendezés (különösen a számítógép) memóriájában elhelyezkedő, azt működtető program;

3.34. *távoli hozzáférés:* a kormányzati megbízható hálózaton kívüli hálózaton (különösen internet) keresztül kommunikáló felhasználó vagy EIR által a rendőri szerv EIR-jéhez való hozzáférés;

3.35. *vagyonelem:* olyan eszköz, adat, információ vagy erőforrás, amely a szervezet számára védendő értéket képvisel.

II. FEJEZET
RÉSZLETES RENDELKEZÉSEK

3. Alapelvek

4. Felhasználó csak az a személy lehet, aki a Rendőrséggel munkavégzésre irányuló jogviszonyban áll, illetve jogszabályi kötelezettség alapján végzi feladatát, továbbá a munkavégzéshez megfelelő informatikai ismeretekkel rendelkezik.
5. A felhasználó köteles az információbiztonság területén az adott helyzetben általában elvárható magatartást tanúsítani, minden károkozó tevékenységtől tartózkodni és az informatikai eszközöket az információbiztonság-tudatosság szem előtt tartásával használni.
6. A munkaköri leírásban úgy kell meghatározni a jogköröket és a feladatköröket, hogy az informatikai eszköz vagy EIR használata során a személyes felelősség megállapításának lehetősége mindenkor biztosított legyen. A munkaköri leírásban feladatkörre szabottan érvényesíteni kell az utasításban foglaltakat.
7. Az EIR-t és annak környezetét alkotó rendszerelemet úgy kell kialakítani, hogy biztosított legyen annak megbízható, rendeltetésnek megfelelő, üzemszerű és folyamatos működése.
8. Az ORFK, valamint a Rendőrség területi és helyi szervei által üzemeltetett vagy felügyelt EIR-ek és azok környezetét alkotó rendszerelemek feladatellátásuk, felhasználásuk tekintetében lehetnek országos hatáskörűek (a továbbiakban: központi EIR), területi hatáskörűek (a továbbiakban: területi EIR) vagy a rendőri szerv által saját használatra üzemeltetett vagy felügyelt EIR-ek (a továbbiakban: helyi EIR).
9. A Rendőrség tulajdonát képező vagy használatában álló eszközöket rendeltetésszerűen, munkavégzés céljából, a Rendőrség érdekeinek szem előtt tartásával, a Rendőrség által meghatározott módon lehet használni. Az eszközök külön engedély nélküli minden egyéb célú, különösen magáncélú használata tilos.
10. Dokumentáltan és a Kiberbiztonsági törvény végrehajtási rendeleteiben meghatározott változáskezelési eljárásnak megfelelő módon kell kezelni minden olyan változtatást vagy hibát, amelynek hatása van vagy lehet az információbiztonságra, így különösen a szervezeti, az információfeldolgozó rendszerelemet és rendszerkonfigurációt, valamint az EIR-t és annak környezetét alkotó rendszerelemet érintő változtatásokat.
11. A felhasználó felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver- és szoftverintegritását. Az integritás sérelmének minősül a rendeltetésellenes használat, a hardveres (különösen egy hardver eltávolítása az informatikai eszközből, illetve alkatrész behelyezése) vagy szoftveres módosítás (különösen program telepítése, módosítása, biztonsági beállítások megváltoztatása).
12. A felhasználó csak a saját azonosítójával jelentkezhet be a Rendőrség hálózatára, másnak a saját hozzáférési adatait nem adhatja át, nem teheti lehetővé, hogy ahhoz más hozzáférjen.
13. Információs, számítástechnikai és telekommunikációs eszközt, adathordozót az informatikai rendszerüzemeltető engedélye nélkül az EIR környezetét alkotó rendszerelemhez csatlakoztatni tilos.
14. A felhasználó köteles a biztonságot támogató szoftverek használatára, azokat az általa használt eszközről nem törölheti le, nem kapcsolhatja ki.
15. A felhasználó kizárólag olyan szoftvereket, programokat használhat, amelyek a szolgálatellátás (munkavégzés) céljából szükségesek és használatuk engedélyezett.
16. A felhasználó köteles az általa tapasztalt hibát, felismert biztonsági eseményt vagy az általa feltárt biztonsági sebezhetőséget haladéktalanul jelezni az informatikai rendszerüzemeltetőnek vagy az EIR üzemeltetőnek, hogy annak elhárítása a lehető leghamarabb megtörténjen.
17. Az üzemeltetésért felelős személy, a fejlesztésért felelős személy, az információbiztonságért felelős személy és minden felhasználó úgy köteles eljárni, hogy az EIR teljes életciklusában megvalósuljon, és biztosított legyen az EIR által kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az EIR és elemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelme.
18. Az információbiztonsággal kapcsolatos követelmények megvalósítását az információbiztonságért felelős személy vagy az információbiztonságért felelős szervezeti elem bármikor ellenőrizheti.

19. A magas biztonsági osztályba sorolt EIR-ek esetében a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendeletben (a továbbiakban: MK rendelet) meghatározott magas biztonsági osztályba tartozó programmenedzsment, a szabályzat, illetve az eljárásrendek követelménycsoportokban meghatározott védelmi intézkedéseket az adott EIR-re vonatkozó normában kell szabályozni, a további követelménycsoportokban meghatározott védelmi intézkedéseket az adott EIR rendszerbiztonsági tervében kell meghatározni.

4. Adatosztályozás

20. Az EIR-ben kezelt adatok osztályozása a Nemzeti Kibervédelmi Intézet (a továbbiakban: Hatóság) által közzétett útmutató alapján a felelős szakterület feladata, amelyben az információbiztonságért felelős személy közreműködik.
21. Az adatosztályozás során fel kell mérni
    a) az EIR-ben kezelt adatok jellegét;
    b) a kezelt adatok mennyiségét;
    c) a bizalmasság, sértetlenség, rendelkezésre állás szempontjából a kompromittálódás esetén bekövetkező kárt és a kár nagyságát.
22. Amennyiben az EIR-ben személyes adatot kezelnek, az adatosztályozásba az adatvédelmi felelőst, annak hiányában az adatvédelmi tisztviselőt is bevonja az illetékes szakterület.

5. Az EIR-ek biztonsági osztályba sorolása

23. Az EIR-ek biztonsági osztályba sorolását az információbiztonságért felelős személy a felelős szakterület és az EIR üzemeltető közreműködésével készíti elő az MK rendelet 1. melléklet 2.2. pontjában foglaltak alapján.
24. Az információbiztonságért felelős személy a felelős szakterület és az EIR üzemeltető közreműködésével a Rendszerbiztonsági Tervben dokumentálja az MK rendelet 3. mellékletében foglalt fenyegetések katalógusa elemeinek vizsgálatával az EIR bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket és azok hatását.
25. Amennyiben a Rendőrség az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe (kiszervezett tevékenységként vagy jogszabály által kijelölt, központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevételével), a biztonsági osztályba sorolásnak megfelelő feltételek teljesülését szolgáltatási szerződés útján kell biztosítani.
26. Ha az EIR létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, a rendőri szerv gondoskodik arról, hogy a biztonsági osztályba sorolásnak megfelelő feltételek szerződéses kötelemként teljesüljenek.
27. Az ORFK által üzemeltetett vagy felügyelt EIR-ek biztonsági osztályba sorolásának előkészítéséről, nyilvántartásba vételéről szóló dokumentumokat az ORFK Hivatal Elektronikus Ügyviteli és Adatvédelmi Főosztály Elektronikus Biztonság Felügyeleti Osztály (a továbbiakban: EBFO) az ORFK Hivatal hivatalvezetőjén keresztül terjeszti fel jóváhagyás céljából az országos rendőrfőkapitány részére.
28. A területi szerv gondoskodik az általa vagy az alárendeltségébe tartozó helyi szervek által üzemeltetett vagy felügyelt EIR-ek biztonsági osztályba sorolásának előkészítéséről és nyilvántartásba vételéről. Az EIR-ek biztonsági osztályba sorolásának eredményéről a Hatóság általi nyilvántartásba vételt követően a területi szerv információbiztonságért felelős személye 30 napon belül tájékoztatja az EBFO-t.
29. Amennyiben az információbiztonságért felelős személy a biztonsági osztályba sorolást követően a biztonsági osztályba sorolás meghatározásánál hiányosságot állapít meg, az EIR üzemeltető közreműködésével eltéréseket vagy helyettesítő intézkedéseket határoz meg, ami biztosítja a biztonsági osztályba soroláshoz tartozó minimális követelményeknek való megfelelést. Az eltéréseket és a helyettesítő intézkedéseket tartalmazó dokumentumokat az MK rendeletben meghatározott tartalommal az EIR-t üzemeltető vagy felügyelő szerv vezetője hagyja jóvá.
30. Az EIR-ek biztonsági osztályba sorolásának eredményéről az információbiztonságért felelős személy naprakész nyilvántartást vezet.

6. Rendszerbiztonsági Terv

31. Az 1. pontban meghatározott szervek által működtetett, üzemeltetett vagy szolgáltatásként igénybe vett EIR esetében Rendszerbiztonsági Tervet kell készíteni és azt naprakészen kell tartani. A Rendszerbiztonsági Terv kidolgozásáért és naprakészen tartásáért az EIR teljes életciklusában, a fejlesztővel, az EIR üzemeltetővel és a felelős szakterülettel együttműködve az 1. pont a) és b) alpontjában meghatározott szervek információbiztonságért felelős személye felel. A Rendszerbiztonsági Tervet a szerv vezetője hagyja jóvá.
32. A Rendszerbiztonsági Tervet frissíteni kell az EIR-ben vagy annak üzemeltetési környezetében történt, biztonságot érintő változások, valamint a védelmi intézkedések értékelése során feltárt kockázatok esetén, de legalább a biztonsági osztályba sorolás felülvizsgálata során, egyeztetve a felelős szakterülettel és az EIR üzemeltetővel.
33. Az információbiztonságért felelős személy biztosítja, hogy a Rendszerbiztonsági Tervben rögzítésre kerüljenek a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedések, hogy a szervezet megfelelően reagáljon a szervezeti műveletek és eszközök, személyek, más szervezetek kockázataira.
34. A Rendszerbiztonsági Tervet az 1. mellékletben meghatározott követelményeknek és tartalmi elemeknek megfelelően, a Hatóság által ajánlott Rendszerbiztonsági Terv sablon alapján kell elkészíteni.

7. Az üzletmenet-folytonossági terv

35. Az üzletmenet-folytonossági terv (a továbbiakban: BCP) az EIR és annak környezetét alkotó rendszerelem elvárt szinten való működését biztosító, nem tervezett, negatív hatású események bekövetkezése esetére vonatkozó eljárások dokumentációja.
36. A BCP-ben meghatározott eljárásoknak biztosítaniuk kell az információbiztonsági követelmények kockázatokkal arányos teljesülését.
37. A BCP jóváhagyásra történő előkészítése, felülvizsgálata és a felhasználók szerepkörüknek megfelelő, folyamatos működésre felkészítő képzése a felelős szakterület feladata, az információbiztonságért felelős személy bevonásával.
38. A BCP-ben az MK rendelet 2. melléklet 7.2. pontjában foglaltakon túl meg kell határozni a kockázatértékelést és kockázatelemzést, amely magában foglalja az MK rendelet 3. mellékletében foglalt fenyegetések katalógusa elemeinek vizsgálatával az EIR bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket és azok hatását.

8. Az információbiztonságot érintő dokumentációk kezelése

39. Az EIR-ek információbiztonsággal kapcsolatos dokumentumait az információbiztonságért felelős személy az erre a célra rendszeresített irányítás-, kockázat- és megfelelés-menedzsment rendszerben (a továbbiakban: Secube rendszer) kezeli. Információbiztonsággal kapcsolatos dokumentum különösen az EIR lista (amely tartalmazza az EIR rövid megnevezését, hivatalos teljes megnevezését, alapfeladatait, szolgáltatásait), a kockázatelemzés dokumentuma, a biztonsági osztályba sorolás eredménye, a Rendszerbiztonsági Terv, a BCP és a sérülékenységvizsgálati dokumentumok.
40. A Secube rendszer frissítését az EBFO felügyeli.

9. Az információbiztonság szervezeti felépítése, szerepkörök, feladat- és hatáskörök, felelősségi szabályok

41. Az EIR-ek és azok környezetét alkotó rendszerelemek egységességének biztosítása és az információbiztonsági elvek érvényesítése az országos rendőrfőkapitány felelősségi körébe tartozik.
42. Az országos rendőrfőkapitány hatáskörébe tartozó, információbiztonsággal kapcsolatos szabályok, döntések előkészítéséről az ORFK Hivatal hivatalvezetője, az ezzel összefüggő biztonságos üzemeltetésről a gazdasági országos rendőrfőkapitány-helyettes gondoskodik.
43. Az EIR-ek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról az ORFK vonatkozásában az országos rendőrfőkapitány, a területi szerv, illetve az alárendeltségébe tartozó helyi szervek vonatkozásában a területi szerv vezetője gondoskodik az általa kinevezett vagy kijelölt információbiztonságért felelős személy útján.

44. Az információbiztonságért felelős személy a Kiberbiztonsági törvényben meghatározottakon túl
    a) felügyeli és ellenőrzi információbiztonsági kérdésekben az informatikai biztonsági előírások teljesítésével összefüggő tevékenységet;
    b) gondoskodik az eltéréseket és a helyettesítő intézkedéseket tartalmazó dokumentumok elkészítéséről;
    c) működtetési korlátozásokat írhat elő a munkaállomások és adathordozók informatikai biztonsági felügyeletével összefüggésben, és ellenőrizheti azok betartását;
    d) információbiztonsági szempontból biztonsági ellenőrzéseket és értékeléseket hajt végre;
    e) kétévente vagy az EIR biztonságát érintő, jogszabályban meghatározott változás esetén soron kívül, dokumentáltan felülvizsgálja az EIR biztonsági osztályba sorolásához tartozó védelmi intézkedéseket;
    f) gondoskodik a biztonsági értékelés eredményeképpen feltárt gyengeségek és hiányosságok kijavítására vonatkozó korrekciós intézkedéseket tartalmazó intézkedési terv elkészítéséről;
    g) gondoskodik a felhasználók dokumentált információbiztonság-tudatossági képzéséről;
    h) tevékenysége során együttműködik az adatvédelmi tisztviselővel, az adatvédelmi felelőssel, a biztonsági vezetővel, a védelmi tiszttel, a kritikus szervezetek ellenálló képességéért felelős vezetővel, az informatikai rendszerüzemeltetővel, az EIR üzemeltetőkkel, valamint a Kiberbiztonsági törvényben és végrehajtási rendeleteiben meghatározott szervekkel;
    i) információbiztonsági szempontból véleményezi az információbiztonságot érintő beszerzéseket és a megkötendő megállapodásokat, illetve javaslatot tehet a már megkötött megállapodások módosítására, amennyiben azok nincsenek összhangban az elvárt biztonsági követelményekkel;
    j) véleményezi az utasítás tárgyi hatálya alá tartozó beruházások információbiztonsági követelményeinek teljesülését, felügyeli azok megvalósítását a beruházás teljes életciklusa során.
45. A Rendőrség információbiztonságát érintő döntések előkészítését szolgáló egyeztetésekre – így különösen informatikai fejlesztések, beszerzések vonatkozásában – meg kell hívni az információbiztonságért felelős személyt.
46. A területi szerv információbiztonságért felelős személyének kinevezéséről vagy kijelöléséről a területi szerv vezetője soron kívül tájékoztatja az ORFK Hivatal hivatalvezetőjét.
47. Az ORFK informatikai rendszerüzemeltetője az ORFK Gazdasági Főigazgatóság Informatikai Főosztály (a továbbiakban: INFO) főosztályvezetője.
48. A központi EIR-ek tekintetében az INFO főosztályvezetője irányítja a Rendőrség informatikai és telekommunikációs üzemeltetési tevékenységét.
49. Az EIR és annak környezetét alkotó rendszerelem üzemeltetése során biztonsági esemény vagy kritikus hibajavítás esetén az infrastrukturális alrendszerek, szolgáltatások működésének ideiglenes vagy időszakos szüneteltetéséről, felfüggesztéséről az informatikai rendszerüzemeltető dönt.
50. A felelős szakterület információbiztonsággal összefüggő feladatai:
    a) a hozzáférés és jogosultság biztosítása iránti igények elbírálása;
    b) a felelősségi körébe tartozó EIR-ekre vonatkozó szakmai döntések meghozatala;
    c) az információbiztonsági követelményekre figyelemmel az információbiztonsági kockázatok felmérése;
    d) a hozzáférést kapott felhasználók adatainak és jogosultságainak naprakész nyilvántartása;
    e) az érintett szakmai folyamatok kidolgozása;
    f) a kivezetés előtt álló, már a napi üzem során nem használt EIR-ek információbiztonsági felügyelete, a kivezetés koordinációja;
    g) az EIR-hez hozzáférést és jogosultságot igénylő felhasználó számára az EIR használatához kapcsolódó, a rá vonatkozó biztonsági szabályok megismerésének biztosítása.

10. A hatósági bejelentéssel kapcsolatos feladatok

51. A területi szerv vezetője a Kiberbiztonsági törvényben meghatározott hatósági bejelentéssel kapcsolatos feladatainak ellátásáról egyidejűleg tájékoztatja az ORFK Hivatal hivatalvezetőjét az általa közzétett szempontrendszer alapján.
52. Az információbiztonságért felelős személy fogadja a kibertérből származó kockázatokra vonatkozóan a nemzeti kiberbiztonsági incidenskezelő központ által küldött figyelmeztetéseket, azokat elemzi és értékeli, szükség esetén megteszi a megfelelő intézkedéseket, és azok végrehajtásáról tájékoztatja az ORFK Hivatal hivatalvezetőjét.
53. Az információbiztonságért felelős személy a biztonsági események felderítése, elhárítása és megelőzése érdekében kapcsolatot tart a nemzeti kiberbiztonsági incidenskezelő központtal.

11. Az információbiztonsági kockázatok kezelése

54. Az információbiztonsági kockázatok kezelésének célja, hogy a Rendőrség képes legyen azonosítani az EIR-ek biztonságát veszélyeztető kockázati tényezőket, és az azonosított kockázatokkal arányos védelmi intézkedéseket dolgozzon ki az EIR védelmének érdekében.
55. A Rendőrség az általa működtetett, üzemeltetett vagy szolgáltatásként igénybe vett EIR működésével kapcsolatos kockázatfelmérését, kockázatelemzését és kockázatkezelését az EIR BCP-jében valósítja meg, a biztonsági osztályba sorolással kapcsolatos védelmi intézkedések értékelése alapján a fennmaradó kockázatok kezelésére vonatkozó intézkedési tervet az EIR Rendszerbiztonsági Terve tartalmazza.

12. Beszámolás az információbiztonsági feladatok végrehajtásáról

56. Az információbiztonságért felelős személy évente, a 2. melléklet szerinti tartalommal, jelentésben értékeli a szervezete – területi szerv esetén a területi és az alárendeltségébe tartozó helyi szervek – információbiztonsági helyzetét (a továbbiakban: éves információbiztonsági jelentés), valamint felülvizsgálja az információbiztonsági szabályzatot.
57. A területi szerv információbiztonságért felelős személye az éves információbiztonsági jelentést felterjeszti a területi szerv vezetőjének. A területi szerv vezetője a részére felterjesztett jelentést a tárgyévet követő év március 31. napjáig megküldi az ORFK Hivatal hivatalvezetőjének.
58. Az éves információbiztonsági jelentésekből készített országos jelentést az ORFK Hivatal hivatalvezetője a tárgyévet követő év április 30. napjáig felterjeszti az országos rendőrfőkapitánynak.
59. Az ORFK információbiztonságért felelős személye a Kiberbiztonsági törvényben és végrehajtási rendeleteiben meghatározott követelmények teljesüléséről a Rendőrség szakterületeitől, a területi és a helyi szervektől tájékoztatást vagy adatot kérhet be.

13. A személyi biztonság

60. Amennyiben nemzetbiztonsági ellenőrzés alá eső munkakört ellátó felhasználó esetén kockázati tényező merül fel, valamennyi hozzáférését és jogosultságát azonnal vissza kell vonni.
61. A felhasználó köteles a Rendőrség által meghirdetett, információbiztonság-tudatosságot fokozó, a fenyegetések felismerésére felkészítő, a jelentési kötelezettségek tudatosítását célzó képzésen részt venni.

14. A beosztás vagy a munkakör változásával kapcsolatos információvédelmi feladatok

62. A beosztás vagy a munkakör megváltozása esetén a szervezeti egység, illetve szervezeti elem vezetője egyidejűleg intézkedik a felhasználó hozzáférésének és jogosultságainak, egyéni hitelesítő eszközeinek felülvizsgálata, illetve visszavonása iránt.
63. A 90 napot meghaladó távollét vagy betegség esetén a felhasználó közvetlen szolgálati elöljárója kezdeményezi a felhasználó hozzáférési jogosultságainak, egyéni hitelesítő eszközeinek megvonását, illetve visszavételét.

15. A fizikai és a környezeti biztonság

64. Az EIR védelmét az EIR biztonsági osztályba sorolásának megfelelő fizikai biztonság kialakításával kell biztosítani. Az EIR fizikai és környezeti védelmi elemeit a Rendszerbiztonsági Tervben kell rögzíteni.
65. Távollét esetén a jogosulatlan hozzáférést megakadályozó módon zárva kell tartani az olyan helyiségeket, ahol informatikai eszközökkel történik a munkavégzés.
66. Új épület építése vagy új helyiség kialakítása esetén fel kell mérni, hogy ott milyen biztonsági osztályba sorolt EIR-eket fognak üzemeltetni, és ennek megfelelően kell a fizikai környezetet kialakítani.
67. Amennyiben a személyes felügyelet nem biztosított, az informatikai erőforrásokat koncentráltan tartalmazó helyiségek bejáratát zárva kell tartani.
68. Azokon az épületeken belül, ahol EIR üzemel, a nap 24 órájában személyi vagy biztonságtechnikai felügyeletet kell biztosítani.
69. A belépési eljárásokat és a belépési jogosultságok rendszerét minden olyan helyiség tekintetében szabályozni kell, ahol EIR vagy annak eleme üzemel.

70. A tűzvédelmi előírásokat annak megfelelően kell kialakítani, hogy az épületben milyen biztonsági osztályba sorolt EIR üzemel.
71. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségeket automatikus működésű oltórendszerrel és szellőztető rendszerrel kell ellátni.
72. Az elektromos és szünetmentes hálózatot, a túlfeszültség-, az érintés- és villámvédelmet, valamint a vészkikapcsoló, továbbá a szükségvilágítást biztosító berendezéseket az adott épületre vonatkozóan annak megfelelően kell kialakítani, hogy az épületben milyen biztonsági osztályba sorolt EIR üzemel.
73. Az energiaellátás biztonsága érdekében – az üzemeltetett EIR-ek biztonsági osztályának figyelembevétele mellett – gondoskodni kell a redundáns automatikus szabályozású áramellátásról (különösen áramellátó generátor, kettős áramszolgáltatás betáplálás), amelynek teljesítménye képes kiszolgálni a számítástechnikai eszközökön túl az azok működéséhez szükséges segédüzemi berendezéseket (különösen a klímaberendezéseket) is.
74. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben szabályozni kell a hőmérséklet és a páratartalom szintjét.
75. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekbe csak az elengedhetetlenül szükséges közműhálózat csatlakozhat. A helyiségen belül nem mehet át víz-, gáz-, csatorna- és egyéb közművezeték, felette és a határoló falfelületek mentén vizesblokkot tartalmazó helyiségrész nem lehet, továbbá biztosítani kell az esetleges vízbetörés érzékelését.
76. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben a nyílászárókat zártságot ellenőrző eszközzel kell ellátni, a belső terek védelmét mozgásérzékelővel kell biztosítani. A védelem ki- és bekapcsolása a bejáraton kívül elhelyezett vezérlővel történhet.
77. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek ablakait betekintés és behatolás ellen védő biztonsági fóliával kell védeni. Ablakok elkerülhetetlen létesítése esetén azok közforgalomtól elzárt területre, belső udvarra kell hogy nézzenek.
78. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben a padlóburkolatoknak, az álpadlónak, a berendezési tárgyaknak antisztatikus kivitelűeknek kell lenniük.
79. Tilos az informatikai erőforrásokat koncentráltan tartalmazó helyiségben annak funkciójától eltérő anyagot vagy eszközt tárolni.
80. Az EIR-ről és annak környezetét alkotó rendszerelemekről magáncélú hang- és képfelvétel készítése tilos.
81. Az adatkommunikációs kábelek fizikai védelme érdekében biztosítani kell, hogy az alkalmazott technológiák védjék a kábeleket mechanikai sérülés, elektromágneses zavarok, illegális rácsatlakozás, szándékos rongálás, szabotázs és lopás ellen.

16. A vagyonelemek nyilvántartása, védelme és ellenőrzése

82. Az informatikai rendszerüzemeltetőnek és az EIR üzemeltetőnek konfigurációs nyilvántartást kell vezetnie, amelyben azonosítható az EIR, az annak környezetét alkotó rendszerelemek és azok paraméterei (a továbbiakban: Konfiguráció nyilvántartás).
83. A Konfiguráció nyilvántartásnak pontosan tükröznie kell az aktuális állapotot, ideértve a szükséges és elégséges licencállományt.
84. Az EIR-ek működtetése, üzemeltetése során kizárólag a Konfiguráció nyilvántartásban szereplő hiteles vagyonelemek használhatók.
85. A vagyonelemek átadása, átvétele, megsemmisítése kizárólag dokumentáltan történhet.
86. A konfiguráció engedély nélküli, a változáskezelési eljárástól eltérő megváltoztatását biztonsági eseményként kell kezelni, és ki kell vizsgálni.
87. Az informatikai rendszerüzemeltető a jogosulatlan rendszerelemek automatikus észlelésére automatizált mechanizmusokat működtet.
88. A létesítményekben munkaszünet idejére el kell zárni a védendő információkat tartalmazó dokumentumokat és adattároló eszközöket.
89. Az eszközök képernyőjén a védendő adatokat úgy szabad kezelni, hogy azok tartalmát illetéktelen személyek ne ismerhessék meg.

17. Az adathordozók védelme

90. Nyilvántartásba vétellel kell biztosítani az adathordozók nyomon követhetőségét, továbbá a személyi felelősség megállapíthatóságát. Az adathordozók nyilvántartásáért az azt felhasználó szervezeti elem vezetője felel.
91. Az adathordozó vírusellenőrzéséről az informatikai rendszerüzemeltető központilag menedzselt rendszerrel gondoskodik.
92. A beépített adathordozóval ellátott eszköz önmagában is adathordozónak tekintendő.
93. Az adatot tartalmazó adathordozókat védeni kell a visszaélésszerű felhasználástól, a megrongálódástól, továbbá el kell látni jogosulatlan hozzáférés elleni védelemmel.
94. Selejtezés alkalmával az adathordozó tartalmát dokumentáltan törölni kell, ezután az adathordozót olyan fizikai roncsolással kell megsemmisíteni, amely kizárja az újbóli használatbavétel lehetőségét. A megsemmisítés végrehajtásáról jegyzőkönyvet kell felvenni. Működésképtelen adathordozó esetén az erre utaló információt a megsemmisítési jegyzőkönyvben kell feltüntetni.
95. A mobil eszközök illetéktelen felhasználásának megakadályozását és a rajtuk tárolt információkhoz, alkalmazáshoz való hozzáférések elleni védelmet a rendőri szerv által üzemeltetett központi menedzsment eszközzel kell biztosítani.
96. Külső adathordozóra másolás előtt a felhasználónak vírusellenőrzést kell végrehajtania a másolandó adatállományon, a forrás-munkaállomáson rendszeresített vírusellenőrző programmal.

18. A hozzáférés és jogosultságok felügyelete

97. Az információhoz és az információt feldolgozó eszközökhöz való hozzáférést korlátozni kell az arra jogosultak körére, figyelembe véve a munkakörökhöz tartozó kockázati besorolást és az átvilágítási kritériumokat.
98. A felhasználó számára csak olyan hálózatokhoz és hálózati szolgáltatásokhoz biztosítható hozzáférés és jogosultság, amelyek használata engedélyezett a számára, feltéve, hogy rendelkezik a szükséges feltételekkel, és megkapta a szerepköréhez és feladatához kapcsolódó képzést. A hozzáférés és jogosultság körét a munkavégzéshez minimálisan szükséges mértékűre kell korlátozni, a szükséges és elégséges ismeret elvének megfelelően.
99. Az EIR-hez történő hozzáférés az EIR biztonsági beállításainak érvényesítését és azok ellenőrzését követően biztosítható. Az EIR-hez történő hozzáférés az EIR biztonsági osztályának megfelelő azonosítás után biztosítható. Az azonosítás személyes használatra kiadott egyedi felhasználói névvel és az ahhoz tartozó, kizárólag a felhasználó által ismert jelszóval és a használt EIR biztonsági osztályának megfelelő további azonosítással történhet. Az előbbiekben meghatározott azonosítással egyenértékűnek kell tekinteni a hardver- vagy szoftveralapú jelszókezeléssel vagy biometrikus adatokkal (különösen arcképmás, ujjnyomat, aláírás) biztosított azonosítást.
100. Az EIR-nek alkalmasnak kell lennie a jogosultságok egyedi vagy csoportszinten való megkülönböztetésére és szabályozására, valamint a felhasználók személyhez köthető, egyedi azonosítására.
101. A felhasználót egyedi azonosítóval kell ellátni, amelynek alapján nyomon követhető az EIR-ben és annak környezetét alkotó rendszerelemben végzett tevékenysége.
102. A jelszókezelés szabályai:
    a) komplex jelszó használat (kisbetű, nagybetű, legalább egy szám és speciális karakter kombinációból legalább három);
    b) minimum jelszóhosszúság: 10 karakter;
    c) 10 elrontott jelszó esetén 30 perc kitiltás;
    d) jelszómódosítási kötelezettség 30 naponta;
    e) utolsó 4 jelszó nem használható újra;
    f) nem visszafejthető, nem visszajátszható jelszókezelés;
    g) két jelszóváltoztatás között 24 órának kell eltelnie.
103. A 102. pontban rögzített szabályoktól eltérő, szigorúbb jelszókezelés az egyes Rendszerbiztonsági Tervekben foglaltaknak megfelelően alkalmazható.
104. A felhasználói jelszó tekintetében a jelszavakra vonatkozó szabályok betartásának ellenőrzésére és érvényesítésére a címtár felhasználóazonosító rendszerét vagy az adott EIR felhasználóazonosító rendszerét kell igénybe venni.
105. A hitelesítési folyamat során a hitelesítési információk visszajelzésekor a hitelesítési információt meg kell védeni a jogosulatlan személyek általi felfedéstől és felhasználástól.
106. A felhasználó az első bejelentkezése után köteles azonnal megváltoztatni a jelszavát. A felhasználónak lehetőséget kell biztosítani arra, hogy jelszavát bármikor megváltoztathassa.

107. A jelszó kompromittálódásának gyanúja esetén a felhasználó haladéktalanul köteles megváltoztatni jelszavát.
108. A Rendőrség által biztosított aktív felhasználói informatikai eszközöket jelszavas védelemmel kell ellátni, és legfeljebb 10 perc inaktivitás után automatikusan zárolni kell.
109. Az EIR üzemeltető az információbiztonság fenntartása érdekében a felhasználó hozzáférését és jogosultságát az érintett EIR tekintetében letilthatja, megvonhatja
    a) ideiglenesen, ha a jelszó kompromittálódásának gyanúja megalapozott;
    b) ideiglenesen, ha a felhasználó megsérti a rá vonatkozó információbiztonsági szabályokat;
    c) ideiglenesen vagy véglegesen, ha a felhasználó hozzáférésének és jogosultságának azonnali letiltására, megvonására kap utasítást a felhasználó állományilletékes parancsnokától vagy a munkáltatói jogkör gyakorlójától.
110. A felhasználó jogosultságának kiadásánál törekedni kell a csoportszintű jogosultságok alkalmazására.
111. Az informatikai szerepkörök és feladatok szervezeti egységre és személyre (véglegesen vagy átmeneti időszakra történő) telepítését úgy kell végrehajtani, hogy a fejlesztési, üzemeltetési, ellenőrzési feladatok ellátásának egymástól való függetlensége biztosított legyen.
112. A nem privilegizált felhasználók számára tiltani kell a következő tevékenységeket:
    a) BIOS-hozzáférés;
    b) hardvertelepítés;
    c) szoftvertelepítés;
    d) hozzáférés a rendszerfájlokhoz (módosítás);
    e) rendszeridő- és dátummódosítás;
    f) naplófájlok módosítása, törlése;
    g) operációs rendszer rendszerbeállításainak megváltoztatása;
    h) felhasználó jogosultságainak megváltoztatása;
    i) szoftverterjesztés;
    j) kártékony kódok elleni védelmi mechanizmusok módosítása, leállítása.
113. Az EIR-nek és annak környezetét alkotó rendszerelemnek meg kell akadályoznia, hogy a nem privilegizált felhasználók az EIR és annak környezetét alkotó rendszerelem üzemeltetéséhez vagy fejlesztéséhez szükséges beavatkozásokat hajtsanak végre, ideértve a védelmi intézkedések kikapcsolását, megkerülését vagy megváltoztatását.
114. A felelős szakterület a felhasználók személyügyi, munkaköri változásai esetén a hozzáférést és a jogosultságokat minden esetben haladéktalanul felülvizsgálja, és indokolt esetben intézkedik a hozzáférés és a jogosultságok módosítására, visszavonására.
115. Az informatikai rendszerüzemeltető a 90 napja nem használt felhasználói fiókot, postafiókot automatikusan felfüggeszti.
116. Az informatikai rendszerüzemeltető a 90 napot meghaladó távollét, betegség esetén a felhasználó hozzáférését felfüggeszti. A hozzáférés és a jogosultságok helyettesítéssel kapcsolatos, ideiglenes megváltoztatása az EIR üzemeltető feladata, a felelős szakterület intézkedése alapján.
117. Az információbiztonságért felelős személy feladata, hogy rendszeres információbiztonsági képzés keretében a felhasználók számára átadja a jelszavak használatával kapcsolatos ismereteket. A felkészítés alkalmával minden felhasználóban tudatosítani kell a helytelen jelszóhasználatból adódó veszélyeket és az ezzel járó felelősséget.
118. Az EIR-hez és annak környezetét alkotó rendszerelemhez, a Rendőrség informatikai rendszeréhez való hozzáférés során közzé kell tenni a használatára vonatkozó figyelmeztetést, amely ismerteti az engedélyezett használat feltételeit, és jelzi, hogy a felhasználó a Rendőrség EIR-ét vagy annak környezetét alkotó rendszerelemét, rendszerét használja, valamint hogy a felhasználói tevékenységet az adatvédelmi szabályoknak megfelelően figyelhetik, rögzíthetik, naplózhatják, továbbá, hogy a jogosulatlan használat fegyelmi, büntetőjogi vagy polgári jogi felelősségre vonással járhat.
119. A távoli hozzáférést a felelős szakterület engedélyezi.

19. A titkosítás

120. Az EIR biztonsági osztályának megfelelő védelmi intézkedésként kriptográfiai mechanizmusokat kell alkalmazni
    a) az informatikai szolgáltatásokhoz kapcsolódó digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének védelmére;

b) az adatátvitel során az adatok jogosulatlan felfedése ellen, kivéve, ha az átvitel más, a Rendszerbiztonsági Tervben meghatározott alternatív fizikai ellenintézkedéssel védett;
c) a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének védelmére;
d) a naplóinformáció és a naplókezelő eszköz sértetlenségének védelmére;
e) a mobil eszközökön tárolt információk bizalmasságának és sértetlenségének védelmére vagy az információk hozzáférhetetlenné tételére.

121. A nyilvános kulcsú infrastruktúra alapú hitelesítés esetén a tanúsítványok érvényességét az EIR üzemeltetőnek ellenőriznie kell.

20. Az üzemeltetés biztonsága

122. Az EIR adminisztrátori dokumentációját az EIR fejlesztőjétől vagy az EIR szállítójától a vele kötött szerződésben kell megkövetelni. Az adminisztrátori dokumentációt csak azon felhasználó számára lehet hozzáférhetővé tenni, akinek ez a munkaköri feladatai ellátásához szükséges.
123. Az EIR üzemeltető az EIR-hez alapkonfigurációt állít össze, és azt dokumentált módon karbantartja.
124. Az EIR és annak környezetét alkotó rendszerelem változtatásáról nyilvántartást kell vezetni, amely visszakereshető és dokumentált módon tartalmaz minden megvalósított változtatást. A változtatások nyilvántartásáról EIR esetén az EIR üzemeltető, EIR környezetét alkotó rendszerelem esetén az informatikai rendszerüzemeltető gondoskodik.
125. Minden, az EIR-ben megvalósított változtatás végrehajtása előtt el kell végezni a változtatás tesztelését. Az EIR konfiguráció megváltoztatása előtt az EIR üzemeltető az új verziót teszteli, a hitelességét ellenőrzi, és a változással kapcsolatosan a Rendszerbiztonsági Tervet frissíti.
126. Az EIR üzemeltető minden, az EIR-ben megvalósított változtatás engedélyezése előtt a változtatás elvégzésének információbiztonságra és az üzletmenet-folytonosságra gyakorolt hatását értékeli. Az EIR-ben változtatást az EIR üzemeltető úgy végezhet el, hogy biztosított legyen az eredeti állapot visszaállíthatósága.
127. A szükséges rendszerteljesítmény biztosítása érdekében az EIR üzemeltető feladata a meglévő erőforrások és a várható kapacitásigények folyamatos monitorozása, optimalizálása és a jövőbeni kapacitásszükséglet előrejelzése.
128. Az EIR üzemeltető feladata a naplózás folyamatos működőképességének biztosítása, monitorozása, naplózási hiba esetén a felelős szakterület értesítése.
129. Az éles üzemi környezet védelme érdekében a fejlesztési és tesztelési környezetet az éles üzemi környezettől el kell különíteni.
130. Az informatikai rendszerüzemeltető és az EIR üzemeltető az általa előre meghatározott önellenőrzési terv alapján az EIR védelme érdekében teszteket, önellenőrzéseket végez. Az éles üzemi rendszerek ellenőrzésére is kiterjedő informatikai önellenőrzések követelményeit és a vizsgálati tevékenységeket úgy kell megtervezni és jóváhagyni, hogy a Rendőrség napi működését ne zavarja.
131. A felhasználónak az észlelt hardverelem-meghibásodást haladéktalanul jelentenie kell az informatikai rendszerüzemeltetőnek.
132. A Rendőrség információt feldolgozó eszközeit a gyártó vagy a forgalmazó előírásai szerint kell karbantartani, folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében.
133. A karbantartásokat és a javításokat dokumentálni kell. Minden bejegyzésnek tartalmaznia kell a dátumot, a karbantartást, javítást végrehajtó személyeket és a végzett tevékenységet, beleértve a telepített, kiszerelt, javított vagy eltávolított elem megnevezését és egyedi azonosító adatait, valamint a végrehajtott informatikai feladatokat is.
134. Az EIR karbantartása vagy javítása kizárólag előre meghatározott, a felelős szakterülettel egyeztetett időpontban történhet.
135. A munkaállomások és szerverek karbantartása során ellenőrizni kell a telepített szoftverek listáját és verzióját, valamint a kritikus és biztonsági frissítések, tanúsítványok állapotát.
136. Az EIR-ek azon elemeire, amelyek esetén a karbantartáshoz szükséges információk vagy szakértelem a Rendőrségen belül nem áll rendelkezésre, az EIR üzemeltetőnek rendelkeznie kell karbantartásra vonatkozó üzemeltetéstámogatási megállapodással.
137. A karbantartásokat és javításokat megelőzően és azok befejeztével – a használatbavétel előtt – az EIR üzemeltetőnek az üzemszerű működéshez szükséges konfiguráció-ellenőrzést kell végrehajtania.
138. Az EIR rendelkezésre állását korlátozó munkálatok felhasználókkal történő közlése az EIR üzemeltető feladata, amelynek során figyelembe kell venni a Rendszerbiztonsági Tervben meghatározott elvárt szolgáltatási szintet.
139. Az EIR rendszerelemének selejtezését az EIR üzemeltetőnek dokumentált módon kell végrehajtania. A selejtezésről minden esetben selejtezési jegyzőkönyvet kell készíteni.

140. Az EIR üzemeltető felelős azért, hogy az eszközök újrafelhasználása esetén a korábbi használatból adódóan adatok ne vesszenek el, illetve az adatok bizalmassága ne sérüljön.
141. Az éles üzemű rendszeren elvégzendő frissítést, módosítást az EIR üzemeltető szabályozott változáskezelési eljáráson keresztül dokumentáltan hajtja végre. A változással kapcsolatban biztonsági hatásvizsgálatot kell végezni, amelynek keretein belül az EIR információbiztonságot érintő dokumentációit is frissíteni kell.
142. Az EIR és annak környezetét alkotó rendszerelemek működéséhez szükséges telepített szoftverekről az EIR üzemeltető naprakész nyilvántartást vezet a konfigurációs nyilvántartás részeként. A nyilvántartás tartalmazza legalább a szoftver megnevezését, verziószámát és azon rendszerelemek listáját, ahol a szoftver beüzemelésre került.
143. Az operációs rendszerek és a felhasználói programok kereskedelmi forrásból beszerzett, jogtiszta, gyártói támogatással rendelkező programok vagy a Rendőrség által fejlesztett vagy fejlesztetett, hitelesített alkalmazások lehetnek. Ettől eltérni a jogtisztaság és a hitelesség kivételével az információbiztonságért felelős személy egyetértésével lehet.
144. Az operációs rendszer, az alkalmazás és a hálózati aktív eszköz szoftver verzióját, valamint biztonsági szintjét tesztelést követően a legmagasabb, gyártói támogatással rendelkező szintre kell hozni. Az ettől való eltérés az informatikai rendszerüzemeltető engedélyével, az információbiztonságért felelős személy tájékoztatását követően lehetséges.
145. A biztonsági beállítások meghatározásánál figyelembe kell venni a Rendszerbiztonsági Terv követelményeit, valamint az egyes gyártók és információbiztonsági szervezetek által kiadott biztonsági megerősítési útmutatókat (hardening guide).
146. Az EIR-t és annak környezetét alkotó rendszerelemeit úgy kell beállítani, hogy a működése során keletkező, nem nyilvános maradvány információk – különösen az átmeneti fájlok – bizalmasságát, sértetlenségét védje.
147. Az új EIR bevezetését megelőzően vagy abban az esetben, ha a már meglévő EIR sérülékenységére vonatkozó információ merül fel, az információbiztonságért felelős személy gondoskodik a sérülékenységvizsgálat kezdeményezéséről. A sérülékenységvizsgálat elősegítése során úgy kell eljárni, hogy a vizsgálat a Rendőrség napi működését ne veszélyeztesse, valamint az az előzetesen jóváhagyott eszközökkel, dokumentáltan legyen lefolytatva.
148. Meglévő EIR esetén a biztonságot közvetlenül veszélyeztető hibákat a lehető leghamarabb javítani kell, vagy korrektív kontroll alkalmazásával csökkenteni kell a kockázatokat. Új EIR esetén feltárt sérülékenység javításáról a használatbavételig gondoskodni kell.
149. A hálózatok ki- és bemeneti pontjait minimalizálni kell, továbbá a ki- és bemeneti pontok adatforgalmát elektronikusan naplózni és a naplófájlokat ellenőrizni kell.
150. Az informatikai rendszerüzemeltetőnek az EIR minden arra alkalmas – megfelelő hardver- és szoftverkörnyezettel rendelkező – elemére jóváhagyott, központilag rendszeresített vírusellenőrző szoftvert kell telepítenie és naprakészen tartania.
151. Az informatikai rendszerüzemeltetőnek a hálózatra csatlakozó eszközök esetében központilag, a hálózatra nem csatlakozó eszközök esetében egyenként kell a vírusellenőrző rendszert felügyelni.
152. Amennyiben kártékony kód elemzése szükséges, az informatikai rendszerüzemeltető biztosítja, hogy a kártékony kódot külön külső adathordozón tárolják, amelyen más tartalom nem lehet. Az adathordozón látható módon fel kell tüntetni, hogy kártékony kódot tartalmaz.
153. Az informatikai rendszerüzemeltető a kéretlen és kártékony kódot tartalmazó elektronikus levelek kiszűrésére olyan központilag menedzselt szűrőt üzemeltet, amely automatikusan központilag frissíti az adatbázisát, és frissíti a rendszert új verziók elérhetővé válásakor.
154. A hatékony biztonsági adatmentés érdekében a munkaállomásokon feldolgozott adatállományokat tárolni kizárólag a szervereken és a központi kiszolgálókon, valamint az adatmentésre szolgáló eszközökön lehet.
155. Az adatokról, a szoftverekről és a rendszerképekről a jóváhagyott mentési és archiválási szabályozásnak megfelelően az informatikai rendszerüzemeltetőnek vagy az EIR üzemeltetőnek dokumentáltan kriptográfiai védelemmel ellátott mentéseket kell készítenie, és visszaállítási teszteket kell végrehajtania.
156. Az informatikai rendszerüzemeltetőnek és az EIR üzemeltetőnek minden olyan adatot mentenie kell, amely az auditálás, az ellenőrzés eszköze lehet (különösen naplófájlok, riportok). Ezeket az adatokat a többi felhasználói, illetve rendszeradattól elkülönítetten kell menteni, és biztosítani kell a mentés sértetlenségét.
157. Az EIR-nek és annak környezetét alkotó rendszerelemeknek naplózniuk kell a felhasználói tevékenységet, valamint a privilegizált felhasználó privilegizált jogosultsággal végzett tevékenységeit, ezzel védelmet biztosítva az ellen,

hogy egy adott személy az általa használt EIR tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.

158. Az EIR-t úgy kell kialakítani, hogy időbélyegeket rögzítsen a naplóbejegyzésekben.
159. A naplózásra becsült mennyiségű naplóesemény Rendszerbiztonsági Tervben meghatározott ideig való tárolásához elegendő méretű tárkapacitást kell biztosítani.
160. A technikai és pénzügyi feltételek rendelkezésre állása esetén automatizált naplóesemény-elemző rendszert kell alkalmazni.
161. Az EIR naplóbejegyzések elemzése az EIR üzemeltető, az EIR környezetét alkotó rendszerelemek naplóbejegyzéseinek elemzése az informatikai rendszerüzemeltető feladata. Az elemzést rendszeresen – ha van, automatikus naplóesemény-elemző rendszer használatával – kell elvégezni úgy, hogy a veszélyes vagy tiltott tevékenységekre és történésekre az EIR üzemeltető vagy az informatikai rendszerüzemeltető megfelelően reagálhasson.
162. Az EIR-t és annak környezetét alkotó rendszerelemek naplózását úgy kell kialakítani, hogy naplózási hiba esetén riasztást küldjön az EIR üzemeltetőnek.
163. A naplózóeszközt, illetve a naplóinformációt meg kell védeni a jogosulatlan hozzáféréstől, törléstől, kiiktatástól vagy módosítástól.
164. Az EIR-eket és azok környezetét alkotó rendszerelemeket úgy kell kialakítani, hogy a személyes adatokkal elektronikus úton végzett adatkezelési műveletek jogszerűsége és ellenőrizhetősége biztosított legyen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény által meghatározott adatok naplózásával kapcsolatban, amely naplót a kezelt adat törlését követően tíz évig meg kell őrizni.

21. A hálózat biztonsága

165. Az informatikaihálózat-üzemeltető (a továbbiakban: hálózatüzemeltető) menedzseli és felügyeli a hálózati aktív és passzív eszközöket. A hálózatmenedzsment segítségével kell megoldani a hálózatok biztonságát és az infrastruktúra védelmét.
166. A hálózatüzemeltető olyan ellenőrző-felügyeleti eszközöket használ, amelyek biztosítják a hálózatokban kezelt és továbbított adatok biztonságát, és megóvják a hálózatot a jogosulatlan hozzáférésektől.
167. A hálózatüzemeltető gondoskodik a hálózatok végpontjain komplex fizikai és logikai védelem alkalmazásáról.
168. A Rendőrség hálózatából más hálózatba csak előre meghatározott és a hálózatüzemeltető által engedélyezett eszközzel és módon szabad csatlakozni.
169. A Rendőrség tulajdonában vagy használatában álló eszközön vezeték nélküli internet (WiFi) vagy hálózati hozzáférési pont (Hotspot) kialakítása belső hálózathoz való hozzáféréssel kizárólag az INFO főosztályvezetőjének engedélyével történhet.
170. A hálózatüzemeltető gondoskodik a hálózati eszközökön a naplózás beállításáról és a hálózati eszközök rendszeridejének a hálózati idő protokollhoz (NTP) történő szinkronizálásáról.
171. A hálózati szolgáltatások biztonsági beállítása, valamint annak ellenőrzése, karbantartása a hálózatüzemeltető feladata.
172. Az EIR működéséhez alkalmazott hálózati szolgáltatás biztonsági jellemzőit a Rendszerbiztonsági Tervben dokumentálni kell. Amennyiben több hálózati szolgáltatás működik a rendszerben, úgy a hálózatüzemeltető biztonsági szempontból ezek egymásra gyakorolt hatását is elemzi.
173. Az EIR-ek összekapcsolását csak az adatforgalom felügyeletét lehetővé tevő és biztonságát garantáló informatikai megoldás közbeiktatásával lehet kialakítani.
174. Az EIR-ek összekapcsolásának feltétele a magasabb biztonsági osztályba sorolt EIR követelményeinek teljesítése.
175. A hálózatüzemeltető az informatikai hálózati környezetről naprakész nyilvántartást vezet, amely legalább az alábbi adatokat, illetve információkat tartalmazza:
    a) a belső/külső rendszerkapcsolatokat;
    b) a valós idejű, felhőalapú kapcsolatokat;
    c) a WiFi-rendszer leírását;
    d) a telefonközpont leírását;
    e) az informatikai hálózat topológiai rajzát (logikai felépítési zónákat, határokat, kapcsolatokat, irányokat).
176. Tilos a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése.
177. A hálózat nem használható az alábbi tevékenységekre:
    a) profitszerzést célzó (különösen kriptovaluta-bányászat), direkt üzleti célú tevékenység és reklám;

b) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információk és programok terjesztése;
c) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybe vevő tevékenység (különösen nem hivatalos körlevelek, hálózati játékok, kéretlen reklámok);
d) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, eszközök és szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása (különösen TCP port scan);
e) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen kezelése, módosítása, elérhetetlenné tétele, törlése vagy bármely károkozásra irányuló tevékenység;
f) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen pornográf anyagok közzététele);
g) hálózati üzenetek, hálózati eszközök hamisítása, olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

178. A hálózatüzemeltető minden hálózati szolgáltatásra meghatározza a biztonsági mechanizmusokat, a szolgáltatási szinteket és a kezelési követelményeket.
179. A hálózatüzemeltető gondoskodik arról, hogy az EIR csak a biztonsági architektúrával összhangban elhelyezett határvédelmi eszközökön, felügyelt interfészeken keresztül kapcsolódhasson külső hálózathoz vagy külső EIR-hez.
180. Az eszközök távdiagnosztikai és konfigurációs portjainak használata csak a hálózatüzemeltető engedélyével, dokumentáltan lehetséges.
181. A hálózatüzemeltető a hálózat külső határán aktív hálózati forgalom vizsgálatára és hálózati támadás felismerésére alkalmas, továbbá az alkalmazások és adatbázisok ellenőrzött hozzáférését biztosító tűzfalat üzemeltet.
182. Minden külső infokommunikációs szolgáltatás használatakor felügyelt interfészt kell működtetni, amelyekhez forgalomáramlási szabályokat kell meghatározni. A szabályok meghatározásánál az alapeseti visszautasításból kell kiindulni. A forgalomáramlási szabályok alóli minden kivételt dokumentálni kell, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt. A hálózatüzemeltetőnek félévente dokumentáltan felül kell vizsgálnia a forgalomáramlási szabályok alóli kivételeket, és el kell távolítania azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.
183. A hálózatüzemeltető a hálózatot túlterheléses – szolgáltatásmegtagadás jellegű – támadásokkal szembeni védelemmel látja el.
184. Az információszolgáltatások, a felhasználók és a rendszerek különböző csoportjait a hálózatüzemeltető a hálózatban elkülöníti.
185. Külön hálózati szegmensbe kell szervezni
a) a fizikai vagy logikai alhálózatban lévő szervergépeket és hálózati eszközöket;
b) az éles üzemi környezetek szervergépeit és hálózati eszközeit;
c) a teszt- és fejlesztői környezet szervergépeit és hálózati eszközeit.
186. A levelezőrendszer kizárólag szolgálati feladatok ellátására használható, az abban tárolt és továbbított levelek a Rendőrség adatvagyonának részét képezik.
187. A Rendőrség elektronikus levelezési címjegyzéke nem szolgáltatható ki a Rendőrség állományába nem tartozó személynek.

22. Az EIR beszerzése, fejlesztése, használatbavétele és fenntartása

188. Az információbiztonságot érintő beszerzések teljes életciklusában az információbiztonsági követelményeknek történő megfelelésről gondoskodni kell.
189. Az EIR információbiztonságát érintő szerződésben az információbiztonságért felelős személy bevonásával meg kell határozni a funkcionális és garanciális biztonsági követelményeket, a dokumentációs követelményeket és a dokumentumok védelmére vonatkozó követelményeket, továbbá meg kell határozni a fejlesztési környezetre és a tervezett üzemeltetési környezetre vonatkozó előírásokat.
190. A szerződéses kötelezettségek meghatározásakor gondoskodni kell arról, hogy a biztonsági szabályok előírása már az EIR tervezése során, az információbiztonságáért felelős személy egyetértésével megtörténjen, és az EIR fejlesztésére ennek alapulvételével kerüljön sor. Az EIR-t e biztonsági előírások igazolt teljesülése esetén lehet használatba venni.
191. Az EIR fejlesztése során a jogszabályi követelmények és az információbiztonságért felelős személy által meghatározott szempontok alapján a fejlesztővel kötött szerződésben elő kell írni, hogy a fejlesztés során

a biztonságos programozás irányelveit kövesse, valamint hogy a fejlesztő előzetesen készítse el vagy aktualizálja a vonatkozó biztonsági követelményrendszert a rendszerspecifikációban.

192. Jogszabály eltérő rendelkezése hiányában az EIR valamennyi elemének használatbavételt megelőző, a biztonsági megfelelőség és hitelesség szempontjainak figyelembevételével történő teszteléséről az informatikai rendszer üzemeltetéséért felelős vezető gondoskodik. A biztonsági feltételeket vagy a hitelességi elvárást nem teljesítő EIR-t alkalmazásba venni, üzemeltetni nem lehet.
193. A Nemzeti Hírközlési és Informatikai Tanácsról, valamint a Digitális Kormányzati Ügynökség Zártkörűen Működő Részvénytársaság és a kormányzati informatikai beszerzések központosított közbeszerzési rendszeréről szóló 301/2018. (XII. 27.) Korm. rendelet 7. §-ában foglalt éves informatikai beszerzési terv és éves informatikai fejlesztési terv elkészítése az informatikai rendszerüzemeltető feladata. A tervekben az információbiztonsággal kapcsolatos beszerzéseket, fejlesztéseket el kell különíteni.

23. A beszállítói kapcsolatok

194. Az EIR-t és annak környezetét alkotó rendszerelemeket érintő megállapodások megkötésekor érvényesíteni kell az információbiztonsági követelményeket, beleértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást és a titoktartási nyilatkozatot.
195. Külső személyek részéről a Rendőrség információs vagyonelemeihez való hozzáférés kockázatát a megkötött megállapodásban dokumentált információbiztonsági követelményekkel kell csökkenteni.
196. A megállapodásban rögzíteni kell a biztonsági követelményeket, a biztonsággal kapcsolatos dokumentációs követelményeket, valamint meg kell határozni az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat.

24. A biztonsági események kezelése

197. A biztonságiesemény-kezelési folyamatra olyan rendszert kell alkalmazni, amely támogatja az alábbi tevékenységeket:
    a) a biztonsági esemény jelentése;
    b) a biztonsági eseménnyel kapcsolatos információk gyűjtése;
    c) tudásbázis kiépítése;
    d) azonnali válaszlépés meghatározása;
    e) azonnali válaszlépés végrehajtása;
    f) átfogó válaszlépés szükségességének meghatározása;
    g) javaslat kidolgozása az átfogó válaszlépésre;
    h) átfogó válaszlépés engedélyezése;
    i) átfogó válaszlépés végrehajtása;
    j) a végrehajtás ellenőrzése;
    k) a biztonsági esemény dokumentálása;
    l) biztonságiesemény-kezelési képességek dokumentált tesztelése;
    m) statisztikai kimutatások készítése.
198. Biztonsági esemény felfedezése vagy gyanúja esetén a felhasználónak az eszközt haladéktalanul le kell választania a hálózatról, és értesítenie kell az informatikai rendszerüzemeltetőt és az EIR üzemeltetőt, akik a halaszthatatlan intézkedések megtételével egyidejűleg értesítik az információbiztonságért felelős személyt.
199. Az információbiztonságért felelős személy a biztonsági eseményről és az azonnali megtett intézkedésekről tájékoztatja az ORFK tekintetében az ORFK Hivatal hivatalvezetőjét, területi vagy helyi szerv tekintetében a területi szerv vezetőjét.
200. Az információbiztonságért felelős személy a biztonsági eseménnyel kapcsolatos információkat begyűjti, tájékoztatja a nemzeti kiberbiztonsági incidenskezelő központot, és intézkedik a biztonsági esemény elhárítására.
201. A BCP-ben előírt tevékenységeket a biztonsági események kezelése során figyelembe kell venni, és az intézkedéseket össze kell hangolni.
202. Az információbiztonságért felelős személy elrendelheti az informatikai rendszerüzemeltető és az EIR üzemeltető számára az átfogó válaszlépés végrehajtását, illetve ellenőrizheti a megvalósítást.
203. Az elektronikus információbiztonsági szabályokat megsértő felhasználó felelősségének kivizsgálására intézkedni kell, amelyre az információbiztonságért felelős személy javaslatot tehet.

25. Az üzletmenet-folytonosság

204. Az EIR üzemeltető felelős azért, hogy rendszerösszeomlás, kompromittálódás vagy hiba esetén az EIR az utolsó ismert állapotba kerüljön helyreállításra, és az utolsó ismert mentésből a tranzakciók is helyreállításra kerüljenek a BCP-ben meghatározottak szerint.
205. A felelős szakterületnek az üzletmenet-folytonosság működésképességének biztosítása érdekében a működtetési környezet jelentős változásakor, de legalább évente, valamint nem tervezett, negatív hatású események bekövetkezése esetén el kell végeznie a BCP dokumentált felülvizsgálatát és tesztelését, az információbiztonságért felelős személy bevonásával. Az EIR üzemeltetőnek az eredmények alapján szükséges javításokat el kell végeznie.
206. Az EIR üzletmenet-folytonosságot befolyásoló szolgáltatásait az adott EIR BCP-jének megfelelő határidőn belül helyre kell állítani.
207. Az EIR biztonsági osztályba sorolásának megfelelően a BCP-ben meghatározottak szerint olyan, az elsődleges feldolgozási helyszíntől elkülönülő tartalék feldolgozási helyszínt kell biztosítani, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésre, az EIR az előre meghatározott műveleteit előre meghatározott időn belül – összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal – a tartalék helyszínen újrakezdhesse vagy folytathassa.

III. FEJEZET
ZÁRÓ RENDELKEZÉSEK

208. Ez az utasítás a közzétételét követő napon lép hatályba.
209. A területi szerv a saját szervezetére és az alárendeltségébe tartozó helyi szervekre vonatkozó információbiztonsági szabályzatot az utasítással összhangban készíti el. A területi szerv az információbiztonsági szabályzatát a Kiberbiztonsági törvényben meghatározott, a Hatóság általi nyilvántartásba vételt követően 30 napon belül tájékoztatásul megküldi az ORFK Hivatal részére.
210. Hatályát veszti az Informatikai Biztonsági Szabályzatról szóló 18/2018. (V. 31.) ORFK utasítás.

Dr. Balogh János r. altábornagy s. k.,
országos rendőrfőkapitány

1. melléklet a 12/2025. (IV. 30.) ORFK utasításhoz

RENDSZERBIZTONSÁGI TERV KÖTELEZŐ TARTALMI ELEMEI

1. Változáskövetési adatok:
   a) dátum;
   b) dokumentumverzió;
   c) változások leírása;
   d) módosító neve.

2. A Rendszerbiztonsági Terv felülvizsgálatának következő tervezett időpontja.

3. Az EIR alapadatai:
   a) megnevezés, verziószám;
   b) tárgyi, személyi hatókör (központi, területi, helyi EIR);
   c) alapfeladatok, alapszolgáltatások;
   d) felelős szakterület;
   e) információbiztonság szempontjából meghatározó jelentőségű rendszerelemek részletezése;
   f) egyedi fejlesztés / dobozos szoftver / kombinált termék (kombinált termék esetén részletezés szükséges);
   g) rendeltetésszerű használatához szükséges licencinformációk (ideértve a rendszertámogatásra vonatkozó adatokat is);
   h) fejlesztő adatai;
   i) EIR működésére, adatkezelésre vonatkozó jogszabályhelyek.

4. Az EIR működési körülményei és más elektronikus információs rendszerekkel való kapcsolatai:
   a) magasszintű architektúraábra és -leírás;
   b) elvárt működés technikai feltételei (ideértve a hálózati feltételeket is), környezeti elvárások;
   c) magasszintű adatkapcsolati diagram (DFD), adatkapcsolatokra vonatkozó elvárások (az interfészek paraméterei, a biztonsági követelmények és a kapcsolaton keresztül átvitt adatok típusa);
   d) monitoring, naplózás ismertetése.

5. Az EIR biztonsági besorolása:
   a) az EIR kockázatelemzése és értékelése az MK rendelet 1. melléklet 2.2. pontja alapján;
   b) az EIR biztonsági osztályba sorolása;
   c) a besorolás időpontja.

6. Az EIR-re vonatkozó védelmi intézkedések, biztonsági követelmények:
   a) jogszabályban meghatározott védelmi intézkedések vagy azokat helyettesítő intézkedések;
   b) jogszabályban nem meghatározott, a felelős szakterület által elvárt további védelmi intézkedések;
   c) intézkedési terv a védelmi intézkedések értékelése alapján a fennmaradó kockázatok kezelésére;
   d) az EIR elvárt működési időszaka;
   e) karbantartás engedélyezett időszaka;
   f) karbantartás ütemezése.

7. Az EIR üzletmenet-folytonossággal kapcsolatos elvárások:
   a) megengedhető-e, és milyen mértékben az adatvesztés;
   b) mennyi az EIR működésének a felelős szakterület által elvárt helyreállítási ideje;
   c) az MK rendelet 3. mellékletében foglalt fenyegetések katalógusa elemeinek vizsgálatával az EIR bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetések és azok hatása.

8. Az EIR üzemeltetés és adattárolás:
   a) az adatkezelésre vonatkozó jogszabályi és technikai elvárások;
   b) a kezelt adatok;
   c) adatfeldolgozás és adattárolás:
      ca) helye,
      cb) adatfeldolgozó neve és elérhetősége,
      cc) adatfeldolgozó igénybevételének jogi háttere;
   d) üzemeltetés:
      da) helye,
      db) üzemeltető neve és elérhetősége,
      dc) üzemeltetési szolgáltatás igénybevételének jogi háttere,
      dd) üzemeltetés SLA paraméterei,
      de) EIR függőségei,
      df) rendszerfelügyelet,
      dg) felhasználói fiókok, jogosultságok és hozzáférés kezelése,
      dh) biztonsági mentés, archiválás,
      di) kapcsolódó és gyártói dokumentációk.

2. melléklet a 12/2025. (IV. 30.) ORFK utasításhoz

AZ ÉVES INFORMÁCIÓBIZTONSÁGI JELENTÉS KÖTELEZŐ TARTALMI ELEMEI

1. Jogszabályi megfelelőség biztosítása

1.1. A szervezet információbiztonsági szabályzata

A jogszabályi megfelelőség biztosításához a szervezet értékelt időszakban hatályos információbiztonsági szabályzatával (a továbbiakban: IBSZ) kapcsolatos adatok:

Az IBSZ száma (norma száma) és a hatálybalépés időpontja	
Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) felé történő bejelentésének időpontja, az NKI határozat száma	
Utolsó felülvizsgálat időpontja, felülvizsgálati dokumentum iktatószáma	
Amennyiben a felülvizsgálat módosítási igényt alapozott meg, úgy az intézkedést módosító norma száma, hatálybalépésének időpontja és az NKI felé történő bejelentés időpontja, az NKI határozat száma	

1.2. Az elektronikus információs rendszer biztonságáért felelős személy

A jogszabályi megfelelőség biztosításához a szervezet információbiztonságért felelős személyt nevez vagy jelöl ki.

Az információbiztonságért felelős személy neve, beosztása, munkaköre, elérhetőségei	
NKI felé történő bejelentésének időpontja	
NKI határozat száma	
Az információbiztonságáért felelős személy végzettségét igazoló dokumentum / szakmai tapasztalatot igazoló dokumentum	

1.3. A szervezet elektronikus információs rendszerei

A jogszabályi megfelelőség biztosításához a szervezet által működtetett elektronikus információs rendszerekkel (a továbbiakban: EIR) kapcsolatos adatok:

Az EIR nyilvántartás, az utolsó felülvizsgálatának időpontja, felülvizsgálati dokumentum és iktatószáma	
Az EIR-ek NKI-hez történő bejelentésének időpontja, az NKI határozat száma	

Amennyiben az EIR nyilvántartásban szereplő EIR-ek biztonsági osztályba sorolásával kapcsolatban eltérésekkel vagy helyettesítő intézkedésekkel teljesítettek a követelmények, az eltérésekkel vagy helyettesítő intézkedésekkel kapcsolatos adatok az alábbiak:

a) EIR megnevezése;
b) elvárt védelmi intézkedés;
c) eltérés vagy helyettesítő intézkedés;
d) indokolás.

Amennyiben a kockázatértékelési jelentésben foglalt észrevételek és javaslatok alapján a szervezet további intézkedéseket vezet be a követelmények teljesítése érdekében, az esetlegesen elkészített intézkedési terv adatai:

a) EIR megnevezése;
b) megvalósított védelmi intézkedés;
c) a védelmi intézkedések értékeléséért felelős szerepkört betöltő személyek;
d) az EIR eltérés vagy helyettesítő intézkedés;
e) döntés a rendszer használatbavételéről vagy használatának folytatásáról.

Az EIR nyilvántartásban szereplő EIR-ek vonatkozásában meg kell adni, hogy készült-e

a) Rendszerbiztonsági Terv;
b) üzletmenet-folytonossági terv.

Az üzletmenet-folytonossági tervek tesztelésére vonatkozóan meg kell adni a helyreállítási tesztelés adatait:

a) EIR megnevezése;
b) üzletmenet-folytonossági teszt tárgya (informatikaiszolgáltatás-kimaradás) és időpontja;
c) a helyreállítás elvárt végrehajtási ideje;
d) a helyreállítás valós végrehajtási ideje;
e) a tesztelés eredményével kapcsolatos megállapítások.

2. Felügyeleti és ellenőrzési feladatok

2.1. Biztonsági események kezelése

Biztonsági események adatai:

a) biztonsági esemény tárgya, típusa, észlelés időpontja, az esemény időpontja;
b) jelentés időpontja az eseménykezelő központ felé;
c) az esemény leírása;
d) hatóköre;
e) azonnali és átfogó válaszlépések.

2.2. Az információbiztonságot tudatosító képzések

A szervezet által dokumentált információbiztonsági képzési tevékenységek adatai (például formája, megnevezése, témája):

a) új belépők információbiztonság-tudatossági képzése;
b) általános információbiztonság-tudatossági képzések;
c) speciális szerepkör alapú információbiztonsági képzések.

2.3. Szerződések információbiztonsági megfelelősége

Ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodnia kell arról, hogy a Kiberbiztonsági törvényben foglaltak szerződéses kötelemként teljesüljenek:

Az érintett időszakban hatályos szerződések száma, tárgya	
Az érintett időszakban megkötött szerződések száma, tárgya	
Az érintett időszakban felülvizsgált szerződések száma	

2.4. Biztonságikockázat-elemzések

A kockázatelemzés

a) tárgya;
b) időpontja;
c) a vizsgálat eredménye;
d) a végrehajtott javítás és annak visszamérésének eredménye.

2.5. Ellenőrzések, auditok adatai (pl. vírusvédelem; alaprendszerek patchelése; operációs rendszerek, virtualizáció, cluster, mentések; a mentések helyreállíthatósága; tűzfalszabályok; naplófájlok stb.):

a) az ellenőrzés/audit tárgya;
b) az ellenőrzés/audit időpontja;
c) az ellenőrzést/auditot végző szerepköre (ellenőr: az információbiztonságért felelős személy; auditor: az informatikai üzemeltetésért felelős vezető);
d) ellenőrzés/audit hatóköre;
e) ellenőrzés/audit eredménye.

2.6. Sérülékenységvizsgálatok adatai

A sérülékenységvizsgálat

a) által érintett EIR;

b) időpontja;

c) típusa (white, grey, black box);

d) eredménye.

2.7. Információbiztonsággal összefüggő további adatszolgáltatás

A jelentés kötelező tartalmi elemein túl a szervezet ebben a részben tüntethet fel minden, az információbiztonsággal kapcsolatos észrevételt, javaslatot, eseményt, amiket fontosnak ítél jelenteni.

III. Közlemények

A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 1/2025. (III. 31.) KKB határozata a 2025 tavaszán várható ár- és belvízi helyzetről szóló tájékoztató elfogadásáról

1. A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság (a továbbiakban: KKB) a jelen határozat mellékletét képző, a 2025 tavaszán várható ár- és belvízi helyzetről szóló tájékoztatót megtárgyalta, és az abban foglaltakat elfogadja.

2. A KKB felhívja a BM Országos Katasztrófavédelmi Főigazgatóság főigazgatóját mint a KKB adminisztratív feladatait ellátó szervezet vezetőjét, hogy a KKB Ügyrend 36. pont j) alpontjának megfelelően gondoskodjon a határozat Hivatalos Értesítőben történő közzétételéről.

Dr. Pintér Sándor s. k.,
KKB elnök

Melléklet az 1/2025. (III. 31.) KKB határozathoz

Tájékoztató a 2025 tavaszán várható ár- és belvízi helyzetről[1]

[1] A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság határozatának mellékletét képező, a 2025 tavaszán várható ár- és belvízi helyzetről szóló tájékoztató a BM Országos Katasztrófavédelmi Főigazgatóság honlapján érhető el, a következő útvonalon: https://www.katasztrofavedelem.hu/26425/vedelmi-igazgatas

A Magyar Munkáspárt 2024. évi pénzügyi kimutatása a pártok működéséről és gazdálkodásáról szóló törvény szerint

Bevételek

			(Adatok ezer forintban)
1.	Tagdíjak		4 881
2.	Központi költségvetésből származó támogatás		0
3.	A párt országgyűlési képviselőcsoportjának nyújtott állami támogatás		0
4.	Egyéb hozzájárulások, adományok		15 951
4.1.	Jogi személyektől (nem pénzbeni juttatás)		
4.1.1.	Belföldiektől (500 ezer Ft feletti hozzájárulás nevesítése)		
4.1.2.	Külföldiektől (100 ezer Ft feletti hozzájárulás nevesítése)		
4.2.	Jogi személyeknek nem minősülő gazdasági társaságoktól		
4.2.1.	Belföldiektől (500 ezer Ft feletti hozzájárulás nevesítése)		
4.2.2.	Külföldiektől (100 ezer Ft feletti hozzájárulás nevesítése)		
4.3.	Magánszemélyektől	15 951	
4.3.1.	Belföldiektől (500 ezer Ft feletti hozzájárulás nevesítése): Munkás Gyula	970	
4.3.2.	Külföldiektől (100 ezer Ft feletti hozzájárulás nevesítése)		
5.	A párt által alapított korlátolt felelősségű társaság nyereségéből származó bevétel		0
6.	Egyéb bevétel		790
Összes bevétel a gazdasági évben			**21 622**

Kiadások

1.	Támogatás a párt országgyűlési képviselőcsoportja számára	0
2.	Támogatás egyéb szervezeteknek	0
3.	Vállalkozások alapítására fordított összegek	0
4.	Működési kiadások	16 034
5.	Eszközbeszerzés	236
6.	Politikai tevékenység kiadása	4 711
7.	Egyéb kiadások	368
Összes kiadás a gazdasági évben		**21 349**

Budapest, 2025. március 10.

Karacs Lajosné s. k.,
gazdasági vezető

A Hivatalos Értesítőt az Igazságügyi Minisztérium szerkeszti.
A szerkesztésért felelős: dr. Bíró Attila.
A szerkesztőség címe: 1051 Budapest, Nádor utca 22.
A Hivatalos Értesítő hiteles tartalma elektronikus dokumentumként a https://www.magyarkozlony.hu honlapon érhető el.