Nemzeti Kiberbiztonsági Akcióterv (2025–2030)

Bevezető

Magyarország Kormánya az 1089/2025. (III. 31.) Korm. határozattal elfogadta *Magyarország Kiberbiztonsági Stratégiáját* (a továbbiakban: Kiberstratégia), és felhívta a kiberbiztonságért felelős biztost, hogy a Kiberstratégia végrehajtása érdekében készítse el a *Nemzeti Kiberbiztonsági Akciótervet (2025–2030)*. A Kiberstratégia és az abból levezetett akcióterv célja, hogy az Alaptörvénnyel, a Nemzeti Biztonsági Stratégiával és a Nemzeti Katonai Stratégiával összhangban kijelölt célokat egységes és összehangolt kormányzati cselekvések révén valósítsa meg a magyar kibertérben.

A kiberbiztonság az állam szuverenitásának és működőképességének alapvető feltétele. Az állam felelőssége kiterjed a szabályozási és intézményi környezet biztosítására, az ellenállóképesség növelésére, a kiberfenyegetések észlelésére, megelőzésére és kezelésére alkalmas rendszer kiépítésére. Ezen túl a magánszektor felelőssége is egyértelműen megjelenik a saját ökoszisztémáinak kiberbiztonsága tekintetében. E felelősség különösen hangsúlyos a digitalizáció erősödésével, amikor a gazdasági és társadalmi működés szinte teljes egésze digitális alapokra helyeződik. Az állam, tehát nemcsak mint szabályozó és védelmező, hanem mint példamutató szereplő is megjelenik a kiberbiztonságban: feladata nem pusztán reagálni a kiberfenyegetésekre, hanem előmozdítani a tudatosságot, innovációt, együttműködést és nemzetközi integrációt.

A Kiberstratégia alapján készült akcióterv átfogó, strukturált és végrehajtható feladatrendszerbe rendezi a kiberbiztonsági célokhoz rendelt intézkedéseket, figyelemmel a hatósági határozattal kijelölt kritikus, valamint az ország védelme és biztonsága szempontjából jelentős szervezetekre is.

Az *I. fejezet* a nemzetközi jelenlét megerősítését célozza, különös tekintettel a nemzetközi jog alkalmazására, a felelős állami magatartás normáinak képviseletére, a bizalomerősítő intézkedések előmozdítására, valamint a NATO, EU és ENSZ kereteiben való aktív magyar részvétel biztosítására. Ezek a feladatok nemcsak diplomáciai és szakpolitikai szinten erősítik hazánk pozícióját, hanem a globális biztonság részévé teszik Magyarország szerepvállalását.

A *II. fejezet* az innováció fokozását állítja középpontba, a hazai kutatás-fejlesztési kapacitások ösztönzése, a kis- és középvállalkozások (a továbbiakban: KKV) és startupok támogatása, a nemzetközi technológiai transzfer elősegítése, valamint a biztonságtudatos innovációs ökoszisztéma kialakítása révén. A kiberbiztonság így nem csupán védekezési mechanizmus, hanem versenyképességi tényező is.

A *III. fejezet* a jogi keretrendszer megerősítésével foglalkozik. A jogalkotási és szabályozási reformok célja, hogy egységes, naprakész és a kockázatarányosságot szem előtt tartó szabályozás álljon rendelkezésre a kibertérben való működés, mozgás biztonságosságának megteremtésére, a kiberfenyegetésekre, -támadásokra való reagálásra, valamint az ehhez kapcsolódó beszerzésekre, tanúsításra és együttműködésre, továbbá, hogy a kibertámadásokra adott válaszlépések nemzeti és nemzetközi jogi megfelelősége biztosított legyen.

A *IV. fejezet* a hazai szervezetrendszer további erősítését célozza. A Nemzeti Kiberbiztonsági Munkacsoport, a Nemzeti Kiberbiztonsági Fórum, az ágazati számítógép-biztonsági és

incidenskezelő csoportok (a továbbiakban: Computer Security Incident Response Team, CSIRT) és a biztonsági műveleti központok (a továbbiakban: Security Operation Center, SOC) szerepe megerősödik, valamint kiemelt figyelmet kap a proaktív kiberképességek fejlesztése, az okosváros projektek kiberbiztonsági követése és a nemzeti felhőszolgáltatási minősítési rendszer létrehozása.

Az *V. fejezet* az információáramlás elősegítésére és az alapvető kiberképességek terjesztésére fókuszál. Ide tartozik az információmegosztási szabályozás, a biztonságos technológiai együttműködések kialakítása, a KKV-k bevonása a kiberbiztonsági ökoszisztémába, valamint egy országos tudásmegosztó központ létrehozása.

A *VI. fejezet* a kibertudatosság fejlesztésére és az utánpótlásképzés fokozására irányul. Az oktatási rendszer minden szintjén megjelenő kiberbiztonsági szemlélet, érzékenyítő programok, felnőttképzési kezdeményezések és a „hibavadász" program megalapozzák az állampolgári és szakmai biztonságtudatosság megerősítését.

A *VII. fejezet* a kiberbiztonsági tanúsítás elterjesztését célozza. A tanúsítási rendszer kiépítése és alkalmazása növeli a bizalom szintjét az infokommunikációs rendszerekben, valamint versenyképesebbé teszi a hazai fejlesztéseket.

A *VIII. fejezet* az ágazati kiberbiztonsági feladatok meghatározásával biztosítja a kritikus szektorok – közigazgatás, honvédelem, egészségügy, mezőgazdaság, világűr, energetika, víziközmű és hulladékgazdálkodás – célzott védelmét. Az egyes ágazatokra szabott intézkedések célja a szolgáltatások folytonosságának biztosítása, az ellátási láncok védelme, a digitális infrastruktúra biztonságának megteremtése, valamint a nemzeti szuverenitás fenntartása.

A *Nemzeti Kiberbiztonsági Akcióterv 2025–2030* így nem csupán a stratégia végrehajtási eszköze, hanem a digitális korszakban való nemzeti reziliencia megerősítésének alappillére. Az állam vezető szerepe és felelőssége ebben a folyamatban kiemelkedő: a kiberbiztonság biztosítása nemcsak nemzetvédelmi, hanem gazdasági, társadalmi és kulturális érdek is.

I. Nemzetközi jelenlét megerősítése

1. **Feladat:** A felelős állami magatartás normáinak érvényesítése a nemzetközi kibertérben
   Felelős: Külgazdasági és Külügyminisztérium
   Közreműködő: kiberbiztonságért felelős biztos, Nemzetbiztonsági Szakszolgálat, Honvédelmi Minisztérium, Miniszterelnöki Kabinetiroda
   Határidő: folyamatos
   Leírás: Magyarország aktív részvételének biztosítása szükséges az ENSZ, EBESZ, EU és NATO kiberbiztonsági munkafolyamataiban, a globális felelős állami magatartás konszenzusos továbbfejlesztése érdekében.

2. **Feladat:** Magyar részvétel fokozása a nemzetközi kiberképesség-építési projektekben
   Felelős: kiberbiztonságért felelős biztos
   Közreműködő: Nemzetbiztonsági Szakszolgálat, Külgazdasági és Külügyminisztérium, felsőoktatási intézmények

Határidő: folyamatos
Leírás: A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági törvény) alkalmazása szempontjából érintett szervezetek támogatása szükséges a nemzetközi kiberbiztonsági és a kiberbűnözés elleni projektekbe való bekapcsolódás során.

3. **Feladat:** Magyar kiberdiplomáciai és szakpolitikai érdekek képviselete EU és NATO szinten
Felelős: Külgazdasági és Külügyminisztérium, Honvédelmi Minisztérium
Közreműködő: Miniszterelnöki Kabinetiroda, Honvéd Vezérkar
Határidő: folyamatos
Leírás: Magyarország stratégiai célkitűzéseinek és érdekeinek hatékony képviselete szükséges az EU, NATO és egyéb nemzetközi kibervédelmi fórumokon.

4. **Feladat:** Részvétel a CSIRT-hálózat és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: European Cyber Crisis Liaison Organisation, EU-CyCLONe) műveleti együttműködésében
Felelős: Nemzetbiztonsági Szakszolgálat, Védelmi Igazgatási Hivatal
Közreműködő: Belügyminisztérium, Katonai Nemzetbiztonsági Szolgálat, Miniszterelnöki Kabinetiroda
Határidő: folyamatos
Leírás: Információcsere és műveleti együttműködés erősítése szükséges a nemzeti CSIRT-hálózattal és az EU-CyCLONe-nal.

5. **Feladat:** Magyar részvétel biztosítása nemzetközi kiberbiztonsági és kiberdiplomáciai gyakorlatokban
Felelős: Külgazdasági és Külügyminisztérium, Honvédelmi Minisztérium, kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Honvéd Vezérkar
Határidő: folyamatos, évente aktualizálva
Leírás: A NATO, EU, ENSZ és EBESZ keretei között zajló kiberbiztonsági gyakorlatok előkészítése és a magyar részvétel koordinációja szükséges.

6. **Feladat:** Kiberbűnözés elleni nemzetközi együttműködés fejlesztése
Felelős: Belügyminisztérium
Közreműködő: Europol, Interpol, kiberbiztonságért felelős biztos, Nemzetbiztonsági Szakszolgálat, Külgazdasági és Külügyminisztérium, Igazságügyi Minisztérium
Határidő: folyamatos
Leírás: Az Europol és Interpol keretében, valamint az USA által kezdeményezett nemzetközi zsarolóvírus-ellenes együttműködésben (CRI) történő aktív magyar részvétel biztosítása szükséges.

7. **Feladat**: Kétoldalú és regionális partnerségek kialakítási lehetőségeinek felmérése és folyamatos vizsgálata
Felelős: Külgazdasági és Külügyminisztérium
Közreműködő: kiberbiztonságért felelős biztos, Honvédelmi Minisztérium, Nemzetbiztonsági Szakszolgálat
Határidő: 2025. december 31., ezt követően folyamatos
Leírás: Az egyes kiberbiztonsági pályázatokon konzorciumi formában történő

elindulási lehetőségek vizsgálata céljából a potenciális nemzetközi partnerek felmérése szükséges.

8. **Feladat:** A nemzetközi jog kibertérben történő alkalmazása vonatkozásában nemzeti szintű értelmezés kialakítása
   Felelős: Külgazdasági és Külügyminisztérium
   Közreműködő: kiberbiztonságért felelős biztos, Honvédelmi Minisztérium, Igazságügyi Minisztérium, Nemzetbiztonsági Szakszolgálat, Miniszterelnöki Kabinetiroda, felsőoktatási intézmények, Katonai Nemzetbiztonsági Szolgálat, Honvéd Vezérkar
   Határidő: 2026. június 30.
   Leírás: A NATO és EU keretrendszerébe illeszkedő nemzeti értelmezés kidolgozása és publikálása szükséges a kibertérre alkalmazandó nemzetközi jog vonatkozásában.

9. **Feladat:** Bizalomerősítő intézkedések fejlesztése multilaterális és regionális keretek között
   Felelős: Külgazdasági és Külügyminisztérium
   Közreműködő: kiberbiztonságért felelős biztos, Belügyminisztérium, Honvédelmi Minisztérium, Nemzetbiztonsági Szakszolgálat, Katonai Nemzetbiztonsági Szolgálat, Honvéd Vezérkar
   Határidő: 2027. szeptember 30.
   Leírás: Jó gyakorlatok kialakítása és tapasztalatcsere szükséges a nem szándékos kiberbiztonsági események és a konfliktusok deeszkalációjának megelőzése érdekében.

II. Innováció fokozása

10. **Feladat:** Kiberbiztonsági startupok támogatási programjának kidolgozása
    Felelős: Nemzetgazdasági Minisztérium
    Közreműködő: kiberbiztonságért felelős biztos, Kulturális és Innovációs Minisztérium, Energiaügyi Minisztérium, Nemzeti Innovációs Ügynökség, felsőoktatási intézmények, kutatóintézetek, Nemzetbiztonsági Szakszolgálat
    Határidő: 2026. december 31.
    Leírás: Célzott támogatási program kialakítása szükséges mesterséges intelligencia, dolgok internete (Internet of Things, IoT), 5G és egyéb innovatív technológiák területén aktív kiberbiztonsági induló vállalkozások és ezeket támogató inkubátorok számára, kiemelten a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. melléklete, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 5. melléklete szerinti ágazatokban kijelölt szervezeteknél.

11. **Feladat:** A kiberbiztonsági technológiai export és import ösztönzése és támogatása
    Felelős: Nemzetgazdasági Minisztérium
    Közreműködő: Magyar Kiberbiztonsági Klaszter, Külgazdasági és Külügyminisztérium, egyéb érintett szakmai szervezetek
    Határidő: 2027. december 31.
    Leírás: A kiberbiztonsági technológiák és szolgáltatások nemzetközi piacra lépésének és hazai bevezetésének támogatása érdekében intézkedni kell a technológiai export és import elősegítésére, különös figyelemmel a nemzetközi kapcsolatépítésre és technológiai transzferre, ezzel erősítve Magyarország ipari és gazdasági versenyképességét a globális kiberbiztonsági szektorban.

12. **Feladat:** A KKV-k, a felsőoktatási intézmények és a tudományos szféra bevonása kiberbiztonsági projektekbe
Felelős: Nemzetgazdasági Minisztérium
Közreműködő: kiberbiztonságért felelős biztos, Magyar Tudományos Akadémia, Nemzetbiztonsági Szakszolgálat, Katonai Nemzetbiztonsági Szolgálat, felsőoktatási intézmények
Határidő: 2027. december 31.
Leírás: Strukturált programot kell indítani a KKV-k, a felsőoktatási intézmények és a tudományos közösségek kiberbiztonsági fejlesztésekbe való bevonására.

III. Jogi keretrendszer megerősítése

13. **Feladat:** Nemzeti kiberbiztonsági kapacitások folyamatos értékelése és fejlesztése
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzeti Kiberbiztonsági Munkacsoport tagjai, Nemzetbiztonsági Szakszolgálat
Határidő: éves jelentési kötelezettség, minden év december 31.
Leírás: A nemzeti kiberbiztonsági képességek és szolgáltatások szintjének folyamatos értékelése és fejlesztési terv kidolgozása szükséges.

14. **Feladat:** Felmérés készítése a Digitális Európa Program (a továbbiakban: Digital Europe Programme, DEP) munkaprogramok nemzeti prioritásainak megalapozására
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzeti Kiberbiztonsági Munkacsoport, Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal, Energiaügyi Minisztérium
Határidő: 2026. február 28.
Leírás: Kérdőíves és szakmai konzultációs alapú felmérés készítése szükséges annak érdekében, hogy a jövőbeli DEP munkaprogramjaihoz Magyarország megalapozott, célzott tagállami javaslatokat tudjon megfogalmazni.

15. **Feladat:** Kibertevékenységekre adott válaszok katonai és jogi protokolljának kidolgozása
Felelős: Honvédelmi Minisztérium
Közreműködő: Külgazdasági és Külügyminisztérium, Miniszterelnöki Kabinetiroda, Miniszterelnökség, Honvéd Vezérkar
Határidő: 2026. március 31.
Leírás: Részletes eljárásrend kidolgozása szükséges arra az esetre, ha egy kibertevékenység fegyveres támadásnak minősül, különös figyelemmel a válaszlépések jogi és katonai koordinációjára.

16. **Feladat:** A piaci szereplők és a kiberbiztonsági szervezetrendszer közötti együttműködés megerősítését szolgáló intézkedési keret kidolgozása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetgazdasági Minisztérium, Közbeszerzési Hatóság, Nemzetbiztonsági Szakszolgálat, Honvéd Vezérkar
Határidő: 2026. június 30.
Leírás: Olyan szakpolitikai és jogalkotási intézkedési terv előkészítése szükséges, amely elősegíti a piaci szereplők és a kiberbiztonsági szereplők közötti strukturált, bizalmi alapú együttműködést, beleértve az adatok és incidensek megosztására, valamint a felhőalapú és szolgáltatásként igénybe vett megoldások kiberbiztonsági

megfelelőségére vonatkozó előírásokat, az európai jogszabályok (Cyber Resilience Act, Cyber Solidarity Act, Cybersecurity Act) mentén.

17. **Feladat:** Kibertérbiztonsági fenyegetések beazonosítási és reagálási eljárásainak fejlesztése, és ehhez kapcsolódó kutatások támogatása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Külgazdasági és Külügyminisztérium, Belügyminisztérium, Honvédelmi Minisztérium, Nemzetbiztonsági Szakszolgálat, Katonai Nemzetbiztonsági Szolgálat, Honvéd Vezérkar, felsőoktatási intézmények
Határidő: 2026. december 31.
Leírás: Szükséges egy olyan eljárásrend kidolgozása, amely a szuverenitást (beleértve a kritikus szervezetek, valamint az ország védelme és biztonsága szempontjából jelentős szervezetek működését) veszélyeztető szereplők azonosítását, felkutatását, felelősségre vonását és a reagálási eljárások, valamint válságspecifikus válaszlépések kialakítását célozza.

18. **Feladat:** Országos kiberhigiéniai alapkövetelmények meghatározása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: szabványügyi testületek, ágazati szövetségek, Nemzeti Kiberbiztonsági Fórum tagjai, Nemzetbiztonsági Szakszolgálat, Honvédelmi Minisztérium
Határidő: 2026. december 31.
Leírás: Rendszeres frissítések, biztonságos jelszóházirendek és egyéb kiberhigiénés intézkedések egységes országos szabályrendszerének kidolgozása, valamint az alapkövetelmények elérését segítő közérthető útmutatók publikálása szükséges.

19. **Feladat:** Kiberműveletek jogi és operatív válaszmechanizmusának standardizálása
Felelős: Miniszterelnöki Kabinetiroda
Közreműködő: Külgazdasági és Külügyminisztérium, Igazságügyi Minisztérium, Honvédelmi Minisztérium, Honvéd Vezérkar, Nemzetbiztonsági Szakszolgálat
Határidő: 2027. június 30.
Leírás: Egy olyan nemzeti szintű protokoll kialakítása szükséges, amely nemzetközi jó gyakorlatokkal összhangban biztosítja az esetalapú válaszadások jogi és operatív egyeztetését, nemzetközi jogi megfeleléssel.

20. **Feladat:** Hardver- és szoftverbeszerzési szabályozás és gyakorlat modernizálása kiberbiztonsági aspektusok beépítésével
Felelős: Közigazgatási és Területfejlesztési Minisztérium, kiberbiztonságért felelős biztos
Közreműködő: Igazságügyi Minisztérium, Nemzetbiztonsági Szakszolgálat
Határidő: 2027. december 31.
Leírás: Közbeszerzések biztonsági szempontjainak felülvizsgálata, különös tekintettel a felhőalapú és mesterséges intelligencia-technológiák beszerzésének akadálymentesítésére, a kiberbiztonsági tanúsításokra és az elérhető kiberbiztonsági tanúsítási sémákra.

IV. Hazai szervezetrendszer megszilárdítása

21. **Feladat:** Okosváros projektek kiberbiztonsági követésére és cselekvési terv kidolgozására irányuló program létrehozása

Felelős: Közigazgatási és Területfejlesztési Minisztérium
Közreműködő: Kulturális és Innovációs Minisztérium, Nemzetbiztonsági Szakszolgálat, önkormányzatok
Határidő: 2026. június 30.
Leírás: Figyelemmel kell kísérni az intelligens városfejlesztési projektek kiberbiztonsági kihívásait, közös elvárásrendszert és szükség esetén cselekvési tervet kell kidolgozni.

22. **Feladat:** Ágazati CSIRT, SOC és Információmegosztási és Elemző Központok (a továbbiakban: Information Sharing and Analysis Center, ISAC) létrehozásának és fejlesztésének ösztönzése
Felelős: kiberbiztonságért felelős biztos
Közreműködő: a Kiberbiztonsági törvény szerinti ágazaton belüli kiberbiztonsági incidenskezelő központot irányító ágazati szervek, Nemzetbiztonsági Szakszolgálat
Határidő: 2026. június 30.
Leírás: Támogatni kell állami forrásokból az ágazati szinten működő incidenskezelő és információmegosztó szervezetek létrehozását, ezek együttműködését és folyamatos fejlesztését.

23. **Feladat:** A Nemzeti Kiberbiztonsági Fórum működésének bővítése a civil szféra bevonásával
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzeti Kiberbiztonsági Fórum tagjai, Nemzetbiztonsági Szakszolgálat
Határidő: 2026. október 31.
Leírás: Erősíteni kell a kormányzaton kívüli szereplők, különösen a civil szervezetek és a piaci szféra részvételét a Nemzeti Kiberbiztonsági Fórum munkájában.

24. **Feladat:** Szakmai fórum létrehozása a feltörekvő technológiák és felhőszolgáltatások kiberbiztonsági vizsgálatára
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, felsőoktatási intézmények és kutatóintézetek, kormányzati innovációs és kiberbiztonsági szervezetek, globális és európai felhőszolgáltatók, magyar hírközlési szolgáltatók, felhasználókat képviselő szervezetek
Határidő: 2026. november 30.
Leírás: Olyan szakmai fórumot kell létrehozni, amely folyamatosan vizsgálja a kiberbiztonság szempontjából releváns felhő- és egyéb feltörekvő technológiákat, eredményeiről rendszeresen tájékoztatja a kiberbiztonsági szabályozásban érintett szervezeteket. A fórum tevékenységének koordinációjára célszerű felkérni egy technológiai iparágat reprezentáló szövetséget, például a Digitális Vállalkozások Szövetségét vagy az alkalmazott tudományokkal foglalkozó kutatóintézetet, a HUN-REN Számítástechnikai és Automatizálási Kutatóintézetet.

25. **Feladat:** A proaktív kiberképességek fejlesztése és a helyzetértékelési képességek erősítése
Felelős: Nemzetbiztonsági Szakszolgálat
Közreműködő: Katonai Nemzetbiztonsági Szolgálat, Magyar Honvédség, Országos Rendőr-főkapitányság, a Kiberbiztonsági törvény szerinti ágazaton belüli incidenskezelő központok

Határidő: 2027. június 30.
Leírás: Erősíteni kell a kibertámadások előrejelzésére, megelőzésére és megszakítására vonatkozó képességeket, a helyreállítási mechanizmusok gyors aktiválásának támogatásával és egy nemzeti kiberbiztonsági kockázatelemzési keretrendszer kialakításával.

26. **Feladat:** Nemzeti, honvédelmi, közigazgatási és külügyi SOC-ok fejlesztése
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Katonai Nemzetbiztonsági Szolgálat, Honvédelmi Minisztérium, Magyar Honvédség, Külgazdasági és Külügyminisztérium, közigazgatási szervek
Határidő: 2027. december 31.
Leírás: Biztosítani kell a kulcsfontosságú kiberbiztonsági központok működését és bevonását a stratégiai, kommunikációs és koordinációs fórumokba.

27. **Feladat:** A Rendőrség kiberbűnözés-ellenes technikai kapacitásainak fejlesztése és a felhőalapú adattárolás kialakítása
Felelős: Belügyminisztérium
Közreműködő: Nemzetbiztonsági Szakszolgálat, NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.), Országos Rendőr-főkapitányság
Határidő: 2027. december 31.
Leírás: A digitális bűnjelek biztonságos gyűjtésére és tárolására szolgáló felhőalapú infrastruktúra kiépítése, valamint az ehhez szükséges eszközpark beszerzése és képzések biztosítása a rendőri nyomozások támogatására.

28. **Feladat:** A Nemzeti Kiberbiztonsági Munkacsoport, a Nemzeti Kiberbiztonsági Munkacsoport Operatív Törzs, a kiberbiztonsági almunkacsoportok és a Nemzeti Kiberbiztonsági Fórum működésének hatékonyságvizsgálata és optimalizálása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzeti Kiberbiztonsági Munkacsoport tagjai, Nemzeti Kiberbiztonsági Munkacsoport Operatív Törzs tagjai, kiberbiztonsági almunkacsoportok tagjai, Nemzeti Kiberbiztonsági Fórum tagjai, Nemzetbiztonsági Szakszolgálat
Határidő: 2028. június 30.
Leírás: Felül kell vizsgálni a kiberbiztonsági testületek hatékonyságát, és szükség esetén pontosítani kell a feladat- és hatásköröket a nemzeti szintű együttműködés javítása érdekében.

V. Információáramlás elősegítése, alapvető kiberképességek fejlesztésének előmozdítása

29. **Feladat:** Mikro- és kisvállalkozások támogatása alapvető kiberbiztonsági szolgáltatásokkal
Felelős: Nemzetgazdasági Minisztérium
Közreműködő: kiberbiztonságért felelős biztos, Kulturális és Innovációs Minisztérium, Energiaügyi Minisztérium, Nemzetbiztonsági Szakszolgálat
Határidő: 2026. március 31.
Leírás: Honlap-konfigurációs és naplózási alapszolgáltatások fejlesztése és biztosítása

az információbiztonsági képességekkel nem rendelkező mikro- és kisvállalkozások részére.

30. **Feladat:** Információmegosztási szabályok és technikai feltételek kialakítása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, piaci és tudományos szereplők
Határidő: 2027. március 31.
Leírás: Meg kell határozni a kibereseményekkel kapcsolatos információmegosztás szervezeti, jogi és technikai feltételeit, elősegítve az egyenszilárdságú védelem kialakítását.

31. **Feladat:** Országos kiberbiztonsági tudásmegosztó platform létrehozása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: minisztériumok, felsőoktatási intézmények, Nemzetbiztonsági Szakszolgálat,
Határidő: 2027. június 30.
Leírás: Olyan országos tudásmegosztó platform kialakítása szükséges, amely összefogja a kutatás-fejlesztés, oktatás, szakpolitika és szabályozás kiberbiztonsági vonatkozású tudását és innovációit.

32. **Feladat:** Gyakorlati ajánlások és ellenőrzési irányelvek kidolgozása a kiberbiztonsági információmegosztás szabályozásához
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzeti Kiberbiztonsági Munkacsoport tagjai, Miniszterelnöki Kabinetiroda, piaci és tudományos szereplők
Határidő: 2027. szeptember 30.
Leírás: A hazai és uniós jogszabályok alapján gyakorlati ajánlásokat és ellenőrzési irányelveket kell kidolgozni a kiberfenyegetésekkel kapcsolatos információk szabályozott megosztása érdekében, kiemelt figyelemmel a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. melléklete, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 5. melléklete szerinti ágazatokban kijelölt szervezetekre.

33. **Feladat:** Automatizált biztonságos információátadási rendszerek fejlesztése SOC, ISAC központok számára
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, SOC, ISAC központok
Határidő: 2028. június 30.
Leírás: Fejlesztési projektet kell indítani a biztonságos, automatizált információátadási megoldások kidolgozására a fenyegetettségek gyors felismerése és kezelése céljából.

34. **Feladat:** Kiberbiztonsági elemző kapacitások nyilvántartásának és mérésének országos rendszere
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzetgazdasági Minisztérium, kiberbiztonsági iparági szereplők
Határidő: 2028. június 30.
Leírás: Egy országos nyilvántartási és értékelési rendszer kialakítása a Kiberbiztonsági törvény alkalmazása szempontjából érintett szervezetek kiberbiztonsági elemző

kapacitásairól, a szinergiák kiaknázása és a válsághelyzeti erőforrás-koordináció támogatása érdekében, sztenderdizált mérési módszerek bevezetésével.

VI. Kibertudatosság erősítése, utánpótlásképzés fokozása

35. **Feladat:** Országos szintű, koordinált kiberbiztonsági tudatosságot növelő kampány kidolgozása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzeti Média- és Hírközlési Hatóság, Belügyminisztérium, közszolgálati médiaszolgáltatók, Nemzeti Kiberbiztonsági Fórum tagjai
Határidő: 2026. március 31.
Leírás: Széles körű, a lakosság különböző célcsoportjait célzó figyelemfelhívó kampányok elindítása a dezinformáció elleni védekezés, valamint a kiberhigiénia, érdekében, a nemzetközi trendek és együttműködések figyelembevételével. A kampánynak a társadalom legszélesebb rétege – így az olyan speciális célcsoportok, mint a gyermekek, idősek, fogyatékossággal élők, mikro- és kisvállalkozások vagy a civil szervezetek – részére is elérhetővé kell válnia.

36. **Feladat:** Oktatási programok indítása az időskorúak és hátrányos helyzetű csoportok számára
Felelős: Kulturális és Innovációs Minisztérium
Közreműködő: kiberbiztonságért felelős biztos, Nemzeti Kiberbiztonsági Fórum tagjai, Nemzetbiztonsági Szakszolgálat, Belügyminisztérium, közszolgálati médiaszolgáltatók
Határidő: 2026. június 30.
Leírás: Speciális, gyakorlatorientált képzések elindítása a kibertér biztonságos használatának elsajátítására a hátrányos helyzetű felnőttek körében.

37. **Feladat:** Kiberbiztonsági képzések fejlesztése és esetleges bővítése a szakképzési és a felsőoktatási szférában
Felelős: Kulturális és Innovációs Minisztérium
Közreműködő: szakképző intézmények, felsőoktatási intézmények, Nemzetbiztonsági Szakszolgálat
Határidő: 2026. június 30.
Leírás: A szakképzésnek és a felsőoktatási intézményeknek általános feladata a kiberbiztonsággal kapcsolatos képzések folyamatos fejlesztése, új kiberbiztonsággal foglalkozó tárgyak bevezetése, esetlegesen új kiberbiztonsági szakirányok, tanfolyamok és gyakorlatorientált képzések, tárgyak indítása és fejlesztése a hallgatók kiberfenyegetésekkel szembeni felkészítése érdekében, különös tekintettel a mesterséges intelligenciához kapcsolódó kihívások kezelésére.

38. **Feladat:** Hazai kiberversenyek megszervezése és magyar csapat részvétele nemzetközi kiberbiztonsági versenyeken
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, felsőoktatási intézmények, Magyar Kiberbiztonsági Klaszter, egyéb érintett szakmai szervezetek
Határidő: 2026. június 30. (hazai verseny), majd évente folyamatosan (nemzetközi részvétel)
Leírás: Országos szintű kiberbiztonsági versenyeket kell szervezni különböző szinteken (általános iskola, középiskola, felsőoktatás) tehetséggondozás és

képességfejlesztés céljából, valamint biztosítani kell a magyar csapatok részvételét rangos nemzetközi kiberversenyeken a nemzeti kiberképességek fejlesztése érdekében.

39. **Feladat:** Köznevelési intézmények számára a kiberfenyegetések észlelésére és ellenük való küzdelemre felkészítő program bevezetése
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzeti Média- és Hírközlési Hatóság, Belügyminisztérium, közszolgálati médiaszolgáltatók, Nemzeti Kiberbiztonsági Fórum tagjai
Határidő: 2026. december 31.
Leírás: A köznevelés minden szintjén kötelezően bevezetésre kerülő felkészítő program kidolgozása és tesztelése a digitális tér biztonságos használatának megalapozása érdekében.

40. **Feladat:** Hazai általános és ágazatspecifikus kibergyakorlatok rendszeres szervezése, kiemelt figyelemmel a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. melléklete, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 5. melléklete szerinti ágazatokban kijelölt szervezetekre
Felelős: kiberbiztonságért felelős biztos
Közreműködő: minisztériumok, Nemzetbiztonsági Szakszolgálat, BM Országos Katasztrófavédelmi Főigazgatóság, egyéb érintett szakmai szervezetek
Határidő: 2026. december 31. (majd évente ismétlődően)
Leírás: A nemzeti kibervédelmi képességek fejlesztése érdekében évente általános és ágazati (pl. egészségügyi, energetikai, pénzügyi, közigazgatási) kibergyakorlatokat kell szervezni, amelyek célja az incidensreagálási képességek tesztelése, az együttműködés erősítése és a válságkezelési eljárások fejlesztése.

41. **Feladat:** A középfokú oktatásban kibertér-használati ismeretek biztosítása és a felsőoktatásban a biztonságtudatosság megerősítése
Felelős: Belügyminisztérium, Kulturális és Innovációs Minisztérium
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzeti Média- és Hírközlési Hatóság, Oktatási Hivatal
Határidő: 2027. december 31.
Leírás: A feladat célja, hogy a köznevelés keretében a középfokú oktatásban résztvevők egységesen elsajátítsák a biztonságos kibertér-használat alapjait, valamint a felsőoktatási programokban megjelenjen a biztonságtudatossági szemlélet, különös figyelemmel a digitális állampolgárságra és a nemzeti ellenállóképességre, a tanulók kiberfenyegetésekkel szembeni felkészítésére.

42. **Feladat:** A biztonságos tervezés-, és programozás témák integrálása informatikai felsőoktatási képzésekbe
Felelős: Kulturális és Innovációs Minisztérium
Közreműködő: felsőoktatási intézmények, Magyar Rektori Konferencia, Nemzetbiztonsági Szakszolgálat
Határidő: 2027. december 31.
Leírás: A kiberbiztonsági szemlélet beépítése az informatikai, mérnöki és kapcsolódó felsőoktatási képzésekbe, figyelemmel a szakember-utánpótlás biztosítására.

43. **Feladat:** Állami „hibavadász” program technikai és szervezeti végrehajtásának biztosítása
Felelős: kiberbiztonságért felelős biztos
Közreműködő: Nemzetbiztonsági Szakszolgálat, Energiaügyi Minisztérium
Határidő: 2027. december 31.
Leírás: A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 18/2024. (XII. 23.) Korm. rendelet alapján „hibavadász” program végrehajtásához szükséges infrastrukturális, jogi és eljárásrendi háttér kialakítása.

44. **Feladat:** Ágazati szintű kiberbiztonsági képzési programok kidolgozása
Felelős: Belügyminisztérium
Közreműködő: kiberbiztonságért felelős biztos, Nemzetbiztonsági Szakszolgálat, Közigazgatási és Területfejlesztési Minisztérium; Miniszterelnöki Kormányiroda; Nemzeti Közszolgálati Egyetem
Határidő: 2027. január 31.
Leírás: Közszolgálati dolgozók számára kiberbiztonsági képzések és tudatosságnövelő programok bevezetése a kiberbiztonsági incidensek megelőzése érdekében, különös figyelemmel a kötelező továbbképzési rendszerekbe történő illeszkedés kialakítására.

45. **Feladat:** A Rendőrség állományának kiberbűnözés elleni képzése megújításának megtervezése és végrehajtása
Felelős: Belügyminisztérium
Közreműködő: Nemzetbiztonsági Szakszolgálat, Országos Rendőr-főkapitányság
Határidő: 2028. december 31.
Leírás: Cél a Rendőrség információs rendszer elleni és az információs rendszer felhasználásával elkövetett bűncselekményekkel foglalkozó állományának rendszeres és korszerű kiberbiztonsági képzési programjainak biztosítása.

46. **Feladat:** Kiberbiztonsági incidenskezelési készségek fejlesztése felsőoktatási gyakorlati programok révén
Felelős: Kulturális és Innovációs Minisztérium
Közreműködő: felsőoktatási intézmények, Nemzetbiztonsági Szakszolgálat
Határidő: 2028. december 31.
Leírás: A feladat célja, hogy a felsőoktatási programok között incidenskezelési gyakorlati programokat és szimulációs gyakorlatokat indítson is megjelenjenek a hallgatók és oktatók felkészültségének növelése érdekében, ezzel támogatva a nemzeti kiberbiztonsági képességek erősítését.

VII. Kiberbiztonsági tanúsítás elterjesztése

47. **Feladat:** Nemzeti kiberbiztonsági tanúsítási rendszer kidolgozása az információs és kommunikációs (a továbbiakban: IKT) termékekre és szolgáltatásokra valamint a felhőszolgáltatásokra
Felelős: Szabályozott Tevékenységek Felügyeleti Hatósága
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzeti Akkreditáló Hatóság, Nemzeti Média- és Hírközlési Hatóság, Nemzetgazdasági Minisztérium, Energiaügyi Minisztérium, kiberbiztonsági iparági szakmai szervezetek
Határidő: 2026. június 30.
Leírás: Olyan egységes és nemzeti szintű tanúsítási rendszer kialakítása szükséges,

amely megfelelő biztonsági garanciát nyújt az IKT termékek és szolgáltatások széles körére. Az EU felhőlapú tanúsítási rendszer (EU Clouds Service Scheme, EUCS) figyelembevételével felhőszolgáltatások nemzeti tanúsítási rendszerének létrehozása, amely támogatja a biztonságos szolgáltatásválasztást, különösen a közszféra és szabályozott szektorok részére.

48. **Feladat:** Kiberbiztonsági tanúsítványok előzetes vizsgálatot követően ütemezett kötelezővé tétele kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. melléklete, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 5. melléklete szerinti ágazatokban kijelölt szervezeteknél
Felelős: Szabályozott Tevékenységek Felügyeleti Hatósága, kiberbiztonságért felelős biztos
Közreműködő: minisztériumok, Nemzetbiztonsági Szakszolgálat, BM Országos Katasztrófavédelmi Főigazgatóság
Határidő: 2027. június 30.
Leírás: Jogszabályi keretrendszer létrehozása, amely kötelezővé teszi a tanúsított IKT-termékek és szolgáltatások használatát a nemzetgazdaság szempontjából alapvető ágazatokban szereplőknél.

49. **Feladat:** Tanúsítási rendszer hatásvizsgálata az infokommunikációs piacra
Felelős: Nemzetgazdasági Minisztérium
Közreműködő: Központi Statisztikai Hivatal, Szabályozott Tevékenységek Felügyeleti Hatósága,
Határidő: évente, első alkalommal 2027. június 30.
Leírás: Az alkalmazott tanúsítási rendszer piaci hatásainak folyamatos értékelése, különösen a hazai IKT-szektor versenyképessége és exportképessége szempontjából.

50. **Feladat:** Felhőszolgáltatások hazai minősítési rendszerének és közbeszerzési integrációjának megvalósítása vagy a meglévő gyakorlatok értékelése az EUCS alapján
Felelős: Szabályozott Tevékenységek Felügyeleti Hatósága, Nemzetbiztonsági Szakszolgálat
Közreműködő: Szabályozási és közbeszerzési hatóságok, egyéb szakmai szervezetek, Nemzeti Akkreditáló Hatóság, Energiaügyi Minisztérium
Határidő: 2027. augusztus 31.
Leírás: Meg kell teremteni a felhőszolgáltatások biztonságáról szóló közösségi tanúsítási rendszer integrációját a hazai viszonyoknak megfelelően. Az EUCS alapján kiadott tanúsítványokat nemzeti szempontból is értékelni szükséges.

VIII. Ágazati kiberbiztonsági feladatok

1. Közigazgatási ágazat

51. **Feladat:** A nemzeti, honvédelmi-, és külügyi kiberbiztonsági incidenskezelő központok, valamint SOC-ok bővítése és fejlesztése
Felelős: Miniszterelnöki Kabinetiroda, Honvédelmi Minisztérium, Külgazdasági és Külügyminisztérium
Közreműködő: kiberbiztonságért felelős biztos, Nemzetbiztonsági Szakszolgálat, Katonai Nemzetbiztonsági Szolgálat, NISZ Zrt.,
Határidő: folyamatos
Leírás: A közigazgatási ágazat kibervédelmének folyamatos megerősítéséhez,

fenntartásához szükséges a fokozódó fenyegetettségekhez igazadó mértékű védelmi képességek biztosítása.

52. **Feladat:** Ágazati kockázatelemzési modell kidolgozása a digitális állami szolgáltatások, valamint az állami adatvagyon védelmére
Felelős: Energiaügyi Minisztérium
Közreműködő: Nemzetbiztonsági Szakszolgálat, NISZ Zrt.
Határidő: 2026. június 30.
Leírás: Olyan egységes kockázatelemzési modell kidolgozása szükséges, amely elősegíti a digitális állami szolgáltatások, valamint az állami adatvagyon biztonságának fenntartását és rendszeres újraértékelését a kritikus infrastruktúrák rendszereinek védelme érdekében.

2. Honvédelmi ágazat

53. **Feladat:** A honvédelemhez kapcsolódó kiberbiztonsággal foglalkozó gazdasági, valamint állami szereplők közötti együttműködés, tapasztalatcsere bizalmi alapú erősítése
Felelős: Honvédelmi Minisztérium
Közreműködők: Katonai Nemzetbiztonság Szolgálat, Honvéd Vezérkar, honvédelmi érdek biztosításához kapcsolódó szakmai szervezetek és gazdasági társaságok
Határidő: folyamatos
Leírás: A honvédelmi ágazat feladataihoz kapcsolódó együttműködés fokozása, tapasztalatcsere, rendezvények, konferenciák formájában. Az ágazaton belüli és azok közötti kommunikáció kiemelt jelentősége érdekében hatékonyság erősítése.

54. **Feladat:** Rendszeres, honvédelmi célokhoz kapcsolódó kibergyakorlatok szervezése
Felelős: Honvédelmi Minisztérium
Közreműködő: Katonai Nemzetbiztonsági Szolgálat, Nemzetbiztonsági Szakszolgálat, Honvéd Vezérkar, Nemzeti Közszolgálati Egyetem
Határidő: 2025. december 31., majd évente ismétlődően
Leírás: Éves gyakoriságú kibergyakorlatok szervezése a honvédelmi ágazat és együttműködő személyi állomány számára, amelyek hozzájárulnak a felkészültség fejlesztéséhez, a nemzetközi együttműködés erősítéséhez, illetve elősegítik a tehetséggondozást és a képességfejlesztést.

55. **Feladat:** Honvédelmi érdek biztosításához kapcsolódó gazdasági társaságok kiberképességének fejlesztése
Felelős: Honvédelmi Minisztérium
Közreműködő: Katonai Nemzetbiztonsági Szolgálat, Nemzetbiztonsági Szakszolgálat
Határidő: 2026. június 30.
Leírás: A nemzeti kiberbiztonsági ellenállóképesség erősítése és fokozása érdekében a honvédelemhez kapcsolódó gazdasági szereplők kiberképességei fejlesztésének támogatása, az állami eszközökkel történő ágazati felügyelet és ellenőrzés biztosítása.

3. IKT és digitális infrastruktúra ágazat

56. **Feladat:** Az állami digitális infrastruktúra egységesítésének ütemezett végrehajtása révén proaktív, öntanuló kibervédelmi megoldások bevezetésének koordinációja
Felelős: Energiaügyi Minisztérium

Közreműködő: Digitális Kormányzati Ügynökség, Nemzeti Kibervédelmi Intézet, IKT-ágazati szakhatóságok
Határidő: 2026. június 30.
Leírás: A cél a mesterséges intelligencia alapú kibervédelmi technológiák széleskörű bevezetése, különös tekintettel az okos eszközökkel összekapcsolt rendszerek védelmére, aminek előfeltétele az állami digitális infrastruktúra konszolidációja, homogénebb struktúra kialakítása.

57. **Feladat:** Biztonsági szabályozási keretrendszer kidolgozása a nyílt internet alapvető jellemzőinek védelmére
Felelős: Nemzetgazdasági Minisztérium
Közreműködő: Nemzetbiztonsági Szakszolgálat, Nemzeti Média- és Hírközlési Hatóság
Határidő: 2028. március 31.
Leírás: A nyílt internet integritásának, bizalmasságának és rendelkezésre állásának fenntartása érdekében egységes, alkalmazható biztonsági követelményeket és jogi-szabályozási keretrendszert kell létrehozni, figyelembe véve a technológiai fejlődést és a nemzetközi normákat.

4. Egészségügyi ágazat

58. **Feladat:** Egészségügyi ágazati tudás- és kompetencia központ létrehozása
Felelős: Belügyminisztérium, Semmelweis Egyetem
Közreműködő: Nemzeti Népegészségügyi és Gyógyszerészeti Központ, Országos Kórházi Főigazgatóság, Országos Mentőszolgálat, Nemzeti Egészségbiztosítási Alapkezelő
Határidő: 2026. január 31.
Leírás: Egy olyan ágazati tudás- és kompetenciaközpont létrehozása szükséges, amely támogatja az egészségügyi ágazat stratégiai kiberbiztonsági tervezését, végrehajtását és folyamatos monitoringját, valamint koordinációs szerepet tölt be annak végrehajtásába.

59. **Feladat:** Egészségügyi szakrendszerek és az egészségügyi dolgok internet eszközei (a továbbiakban: Internet of Medical Things, IoMT) kiberbiztonságának növelése nyilvántartások és auditok révén
Felelős: Belügyminisztérium
Közreműködő: Országos Kórházi Főigazgatóság, Nemzeti Népegészségügyi és Gyógyszerészeti Központ, Egészséginformatikai Szolgáltató és Fejlesztési Központ Nonprofit Kft., egészségügyi gyártók, és szolgáltatók
Határidő: 2026. január 31.
Leírás: Az IoMT eszközök országos nyilvántartásának kialakítása, rendszeres auditálása, sérülékenység-adatbázis létrehozása, és az európai szabványosítási eljárásokhoz való kapcsolódás biztosítása szükséges.

60. **Feladat:** Ágazati információbiztonsági megfelelőségi keretrendszer kialakítása az egészségügyi szereplők számára
Felelős: Belügyminisztérium
Közreműködő: Nemzeti Népegészségügyi és Gyógyszerészeti Központ, Egészséginformatikai Szolgáltató és Fejlesztési Központ Nonprofit Kft, Országos Kórházi Főigazgatóság, Országos Mentőszolgálat, egészségügyi szolgáltatók
Határidő: 2026. június 30.
Leírás: Cél egy olyan egységes megfelelőségi keretrendszer kidolgozása, amely az e-

health ökoszisztéma szereplői számára kötelező, és figyelembe veszi a kritikus információbiztonsági és kibervédelmi elvárásokat.

61. **Feladat:** Egységes kiberbiztonsági célú egészségügyi mesterséges intelligencia által támogatott adatkezelési keretrendszer kidolgozása
Felelős: Belügyminisztérium
Közreműködő: Nemzeti Adatvagyon Ügynökség, Egészséginformatikai Szolgáltató és Fejlesztési Központ Nonprofit Kft, Nemzeti Népegészségügyi és Gyógyszerészeti Központ, Országos Kórházi Főigazgatóság, Országos Mentőszolgálat, Nemzeti Egészségbiztosítási Alapkezelő, egészségügyi adatkezelők
Határidő: 2026. december 31.
Leírás: A cél az egészségügyben alkalmazott mesterséges intelligencia-alapú rendszerek működését szabályozó, egységes adatvédelmi és információbiztonsági keretrendszer kialakítása, amely biztosítja az adatvezérelt fejlődés során a bizalom és a biztonság fenntartását.

5. Agrárágazat

62. **Feladat:** Kiberbiztonsági kockázatcsökkentési keretrendszer kidolgozása a mezőgazdasági digitális szolgáltatásokra
Felelős: Agrárminisztérium
Közreműködő: kiberbiztonságért felelős biztos, Nemzetbiztonsági Szakszolgálat
Határidő: 2026. június 30.
Leírás: A feladat célja, hogy szabályozási, szerződéses és technikai eszközökkel csökkentse a hazai mezőgazdaságban elterjedt, külföldi agrárdigitalizációs szolgáltatók által jelentett kockázatokat, különös tekintettel a felhőalapú rendszerekre és a vezérlési utasítások integritására. Ennek keretében külön figyelmet szükséges szentelni a kiemelten kockázatos szolgáltatásoknak (pl. meteorológiai szolgáltatások, navigációs szolgáltatások, gépoptimalizálási szolgáltatások, farmmenedzsment-rendszerek).

6. Világűr ágazat

63. **Feladat:** Kibervédelmi ellenállóképesség növelése az űrszektor értékláncában
Felelős: Nemzetgazdasági Minisztérium
Közreműködő: Kulturális és Innovációs Minisztérium, kiberbiztonságért felelős biztos, Nemzetbiztonsági Szakszolgálat, Külgazdasági és Külügyminisztérium, Honvéd Vezérkar, Honvédelmi Minisztérium, Katonai Nemzetbiztonsági Szolgálat
Határidő: 2026. március 31.
Leírás: Átfogó kibervédelmi keretrendszer kidolgozása szükséges az űrszektor teljes értékláncára, különös tekintettel a beszállítói, szolgáltató és felhasználói szintek sebezhetőségeinek csökkentésére, összhangban a készülő uniós űrjogszabállyal és a NIS2 irányelvvel.

7. Energetika, víziközművek és hulladékgazdálkodás

64. **Feladat:** Hulladékgazdálkodási kiberbiztonsági követelményrendszer kidolgozása és bevezetése
Felelős: Energiaügyi Minisztérium
Közreműködő: Nemzetbiztonsági Szakszolgálat, Országos Hulladékgazdálkodási Hatóság, hulladék-gazdálkodási létesítmény üzemeltetők
Határidő: 2026. március 31.
Leírás: A hulladékgazdálkodás digitalizációja és az egyes létesítmények kritikus szerepe miatt szükséges az ágazati kiberbiztonsági követelmények kialakítása, különös

tekintettel az égetők, feldolgozók és logisztikai rendszerek védelmére, valamint az incidenskezelési együttműködés erősítésére.

65. **Feladat:** Víziközmű-rendszerek kibervédelmi ellenállóképessége minimumkövetelményeinek kidolgozása
Felelős: Energiaügyi Minisztérium
Közreműködő: Magyar Energetikai és Közmű-szabályozási Hivatal, Nemzetbiztonsági Szakszolgálat, víziközmű-szolgáltatók
Határidő: 2026. december 31.
Leírás: Az ivóvíz- és szennyvízszolgáltatások területén terjedő digitális rendszerek kibervédelmi szintjének biztosítása érdekében szabályozási és műszaki minimumkövetelmények meghatározása szükséges már a tervezési szakaszban, figyelemmel azok nemzeti kritikus infrastruktúra jellegére, valamint szükséges a jelenlegi rendszerek kiberbiztonsági célú felülvizsgálata.

66. **Feladat:** Energetikai SOC központok országos hálózata kialakításának és működtetésének támogatása és felügyelete
Felelős: Magyar Energetikai és Közmű-szabályozási Hivatal
Közreműködő: Energiaügyi Minisztérium, Nemzetbiztonsági Szakszolgálat, elosztóhálózat üzemeltető engedélyes vállalkozások
Határidő: 2027. június 30.
Leírás: A villamosenergia-hálózat digitális védelme érdekében szükséges egy központi felügyeleti, elemző és beavatkozásra képes SOC hálózat kialakítása, amely alkalmas a különféle szintű és típusú infrastruktúrák (nagy-, közép- és kisfeszültségű hálózatok, háztartási méretű kiserőművek) valós idejű megfigyelésére és a gyors válaszadásra.