Szakpolitikai szempontok Útmutató

Az elektronikus információbiztonságra vonatkozó követelmények

NEMZETI KIBERVÉDELMI INTÉZET

2025

Tartalomjegyzék

AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGRA VONATKOZÓ KÖVETELMÉNYEK

ÉRTELMEZÉS

A **Digitális Megújulás Operatív Program Plusz** keretében az elektronikus információs rendszer (a továbbiakban: EIR) kialakítására, bővítésére vagy átalakítására irányuló projekt megvalósítása során a Kedvezményezett köteles az EIR biztonságára vonatkozó jogszabályi követelményeknek való megfelelést biztosítani és ennek érdekében a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel (a továbbiakban: NBSZ NKI, Hatóság) együttműködni.

Az információbiztonsággal kapcsolatos követelmények, információk, közlemények a Hatóság honlapján a Hatóság / DIMOP követelmények menüpont alatt találhatók. A honlapon publikált sablonok támogatják a Kedvezményezetteket, valamint általános érvényű elvárások kerültek megfogalmazásra, amelyeket a Kedvezményezetteknek projektspecifikus módon szükséges kiegészíteni, különös tekintettel saját környezetük jellemzőire és a jogszabályok által támasztott követelményekre.

A Megvalósíthatósági Tanulmányban foglalt fejlesztések **információbiztonsági követelményeknek** történő megfeleléséről a Hatóság a támogatási kérelem értékelése, valamint a támogatási jogviszony további fázisai során több alkalommal is szakpolitikai állásfoglalást bocsát ki. **A projektgazdának a Hatósági állásfoglalások észrevételeit, kifogásait a dokumentációban figyelembe kell venni, illetve a fejlesztés során meg kell valósítani.**

A projekt keretében létrehozott EIR biztonsági megfelelősége, az NBSZ NKI által megállapított hiányosságok pótlása, valamint a kockázatkezelési intézkedések meghozatala kapcsán készített szakmai beszámoló **NBSZ NKI általi elfogadása a projekt fejlesztési fázisai lezárásának és az üzembe helyezésnek a feltétele.**

A projekt tervezési fázisában az információbiztonsági szakpolitikai szempontoknak való megfeleléssel kapcsolatos dokumentumokat a **Hatósággal konstruktívan együttműködve úgy szükséges megküldeni, hogy a Hatóság információbiztonsággal kapcsolatos elvárásai az EIR fejlesztésére irányuló szerződésében rögzítésre kerülhessenek.**

⚠ **A Magyarország kiberbiztonságát megalapozó jogszabályok köre 2025. január 1-től megújult**. A 2025. január 1-től hatályos új kiberbiztonsági jogszabály, a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.), valamint a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Vhr.) jelentős változásokat hozott. A hatályos jogszabályok a Hatóság honlapján a Hatóság / Jogszabályok menüpont alatt találhatók.

⚠ A **Kiberbiztonsági tv**. 86. § (1) bekezdésében foglaltak alapján – a Kedvezményezett a Kiberbiztonsági törvény 1. §-ában meghatározott hatály alá tartozástól függően – a fejlesztendő EIR 4 **vonatkozásában a törvény vonatkozó előírásait kell alkalmazni a hatálybalépésekor még használatba nem vett,**

a) saját fejlesztésű EIR esetében, amennyiben az erőforrásigényeket még nem fogadták el,

b) külső fejlesztés alatt álló EIR esetében, amennyiben a fejlesztésre irányuló beszerzési eljárást még nem írták ki, vagy a fejlesztésre irányuló szerződést még nem kötötték meg.

Amennyiben a fenti fázison a törvény hatályba lépésekor már túljutott a Kedvezményezett, akkor a Kiberbiztonsági tv. 86. § (2) bekezdés alapján:

a) a szervezet – ha még nem végezte el, – 180 napon belül elvégzi az elektronikus információs rendszer biztonsági osztályba sorolását,

b) az informatikáért felelős miniszter rendeletében előírt védelmi intézkedések teljesítésénél lehetősége van a 10. § (6) bekezdése szerinti fokozatos kivitelezésre, azzal, hogy a vonatkozó határidő számításának alapját e törvény hatálybalépésének napja képezi.

⚠ Azon Kedvezményezettek, akik a Kiberbiztonsági törvény hatálybalépésekor még használatba nem vett EIR vonatkozásában a fejlesztésre irányuló beszerzési eljárást kiírták, vagy a fejlesztésre irányuló szerződést megkötötték a Kiberbiztonsági tv. hatálybalépését megelőzően és a fejlesztendő EIR vonatkozásában rendelkeznek – ideértve különösen az ITB műszaki ellenőr alkalmassághoz, a biztonsági osztályba soroláshoz, az Információbiztonsági tervhez, a Rendszerbiztonsági tervhez kapcsolódóan – a Hatóság által elfogadott döntéssel, úgy azokat nem szükséges a jogszabályi változásoknak megfelelően átdolgozni és ismételt ellenőrzésre benyújtani.

⚠ A jogszabályi változások értelmezéséhez tekintse meg a Hatóság honlapjának Hatóság / Hatályos hatáskör menüpontja alatt található segédleteket!

⚠ A Kiberbiztonsági tv. a 13-15 §-okban a rendszerek fejlesztésével és továbbfejlesztésével kapcsolatos elvárásokat fogalmaz meg. Abban az esetben, ha a kedvezményezett, vagy a fejlesztendő rendszer felett rendelkezést gyakorló szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) hatálya alá tartozik, akkor ezek a DIMOP szakpolitikai elvárásokkal párhuzamosan teljesítendő előírások. Ez a gyakorlatban azt jelenti, hogy a hatósági jóváhagyások érdekében a szükséges dokumentumokat a Hatóság számára a jogszabályban meghatározott formában és csatornán is be kell nyújtani, melyek tekintetében a szakpolitikai állásfoglalásokon túlmenően a Hatóság formális döntéseket is hoz. Ezekben az esetekben a jogszabályban meghatározott kapcsolattartási csatorna a Hatóság Hivatali kapuja.

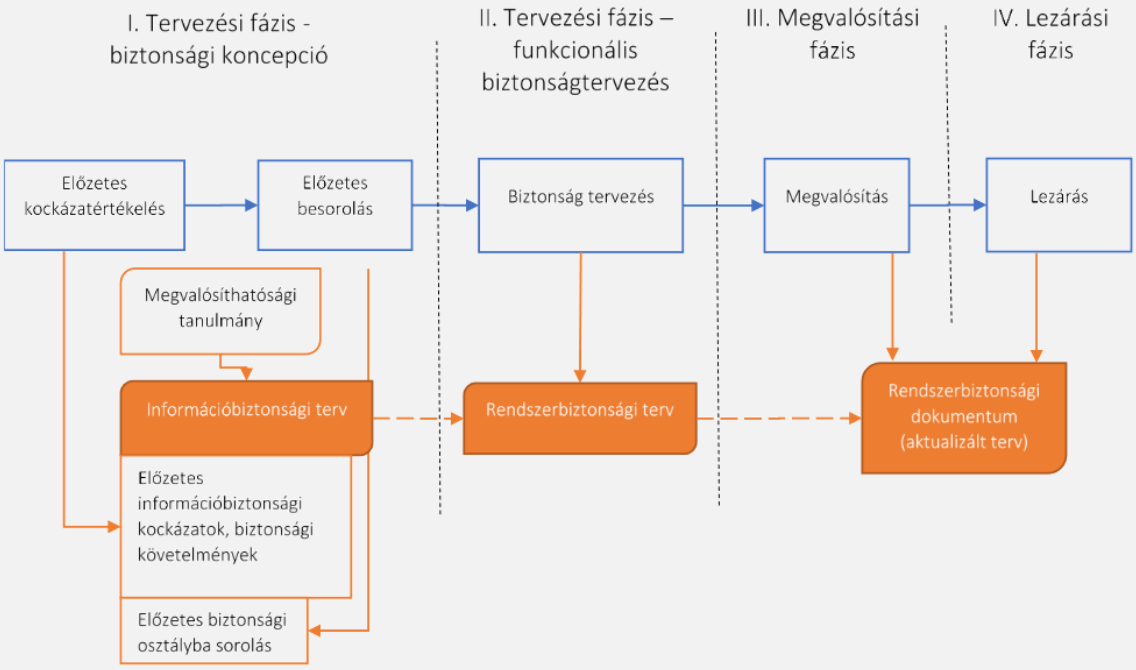
A projektet érintő – információbiztonsággal kapcsolatos – kérdésekkel, észrevételekkel kapcsolatban segítség a dimop@nbsz.gov.hu e-mail címen, illetve a +36 (1) 206-9320-as központi telefonszámon (hivatali munkaidőben) kérhető.

Általános elvárások

- Az elektronikus információbiztonsághoz kapcsolódó – a lenti fejezetekben részletezett – fejlesztési fázisokhoz rendelt eredménytermékeket mérföldkövekhez rögzítetten szükséges tervezni a projekt Megvalósíthatósági Tanulmányában.
- A projekt megvalósulásának keretében az EIR kialakítására, bővítésére vagy átalakítására irányuló fejlesztés megkezdésének feltétele a Hatóság által elfogadott ITB műszaki ellenőr (az ITB műszaki ellenőrre vonatkozó alkalmassági feltételek az NBSZ NKI honlapján megtalálhatók).
- Legkésőbb az EIR létrehozásával, vagy fejlesztésével kapcsolatos (köz)beszerzési eljárások megindításáig rendelkezésre kell állnia a Hatóság által elfogadott, az Információbiztonsági Terv részeként elkészített előzetes kockázatelemzésnek, amelynek tartalmaznia kell a fejlesztett EIR átadása előtti kockázatértékelési szempontokat is. El kell készíteni a megfelelő hatáselemzésen alapuló előzetes biztonsági osztályba sorolást, valamint a jogszabályban meghatározott esetekben az adatosztályozást is.
- A projektek megvalósítása folyamán az információbiztonsággal kapcsolatos műszaki, szakmai tartalmat érintő lényegi módosításokat szükséges az NBSZ NKI részére bejelenteni. Lényegi módosításnak kell tekinteni minden, az NBSZ NKI által véleményezett és/vagy jóváhagyott információbiztonsággal kapcsolatos dokumentumban bekövetkező tartalmi változtatást (ideértve különösen az ITB műszaki ellenőr személyét, az előzetes biztonsági osztályba sorolás dokumentumait, az Információbiztonsági tervet, a Rendszerbiztonsági tervet érintő változásokat). Az NBSZ NKI a projekt ütemezésben bekövetkezett esetleges változásokat szakmai szempontból értékeli. Az értékelés alapján válik megítélhetővé, hogy az lényegi módosítás-e.

A projektek fejlesztési fázisai: az IT biztonsággal kapcsolatos feladatok szakaszai és eredménytermék

A projektek megvalósítása folyamán az információbiztonsági elvárások teljesülése nem a projekthez kapcsolódó Felhívás 5. pontja (Mérföldkövek, indikátorok) szerinti mérföldkövekhez, hanem a jelen Útmutató szerinti fázisokhoz van rendelve az alábbiak szerint:



Egy-egy fázisnál meghatározott elvárások, szakmai eredmények együttes teljesülése járul hozzá a Felhívásokban megfogalmazott szakpolitikai szempontoknak való maradéktalan megfelelésnek. A fent megjelölt **fázisok nem független időszakok, mind egymással, mind a projekt mérföldköveivel szinergiában állnak.**

⚠ A mérföldkövet lezáró, a 2021–2027 programozási időszakban az egyes európai uniós alapokból származó támogatások felhasználásának rendjéről szóló 256/2021. (V. 18.) Korm. rendelet 294. § (1) bekezdés szerinti műszaki-szakmai beszámolóban meg kell jeleníteni az információbiztonsági elvárások előrehaladását – összhangban az ITB műszaki ellenőri adatszolgáltatás tartalmával –, függetlenül az adott fázis készültségi fokától.

Tervezési fázis – biztonsági koncepció:

Azon projektek esetében, melyeknél 2025. január 1-je előtt a fejlesztésre irányuló beszerzési eljárást még nem írták ki, vagy a fejlesztésre irányuló szerződést még nem kötötték meg a Kedvezményezett köteles az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet) szerinti kritériumrendszer mentén meghatározni a projekt keretében fejlesztéssel érintett EIR biztonsági osztályát a projekt tervezési időszakában.

⚠ A Kiberbiztonsági tv. 13. § (3) bekezdésben foglaltak alapján a fejlesztendő EIR biztonsági osztályba sorolását a **Vhr-ben meghatározott módon** a Hatóságnak jóváhagyásra be kell nyújtani legkésőbb

a) belső fejlesztés esetén az erőforrások allokációját megelőzően,

b) külső fejlesztés esetén az arra irányuló szerződés megkötését megelőzően – a közbeszerzésekre vonatkozó jogszabályi rendelkezéseket is figyelembe véve – olyan módon, hogy az információbiztonsági követelmények az EIR fejlesztésére irányuló szerződésbe rögzítésre kerüljenek.

Az Információbiztonsági terv célja az EIR tervezéséhez kapcsolódó, a fejlesztéssel kapcsolatos biztonsági előírások és funkciók bemutatása, a Rendszerbiztonsági terv elkészítésének elősegítése, összhangban a hatályos jogszabályokban és a Kedvezményezett belső szabályzataiban foglaltakkal.

A Kedvezményezett feladatai:

- Az MK rendelet szerinti kritériumrendszer mentén meg kell határozni a fejlesztéssel érintett EIR(ek) biztonsági osztályát (Elozetes-besorolast-tamogato-utmutato.docx), valamint a jogszabályban meghatározott esetekben az adatosztályozást is végre kell hajtani.
- Az NBSZ NKI ajánlása alapján Információbiztonsági tervet kell készíteni. (Informaciobiztonsagi- terv-sablon.docx).
- Az NBSZ NKI ajánlása alapján előzetes kockázatelemzést (kockázat-kárérték meghatározást) kell készíteni (https://nki.gov.hu/it-biztonsag/tudastar).
- Az elektronikus információbiztonsághoz kapcsolódó, a fejlesztési fázisokhoz rendelt eredménytermékeket mérföldkövekhez rögzítetten szükséges tervezni a Megvalósíthatósági Tanulmányban.
- Megfelelő képzettséggel, képességekkel és tapasztalattal rendelkező ITB műszaki ellenőrt kell alkalmazni a biztonsági szempontok érvényre juttatása érdekében (ITB-muszaki-ellenor_2025.docx).

⚠ Az ITB műszaki ellenőr alkalmasságát az NBSZ NKI irányába igazolnia kell az dokumentumok elektronikus megküldésével (Hivatali kapu: NBSZ [KRID: 427386978]). Az ITB műszaki ellenőr személyét az NBSZ NKI-nak jóvá kell hagynia, vagy ha az alkalmasság egyértelműen nem megállapítható, a Hatóságnak hiánypótlást kell küldenie az alkalmasságot igazoló dokumentumok elektronikus megküldését követő 15 munkanapon belül.

⚠ A Hatóság az előzetes kockázatértékeléssel, az előzetes biztonsági osztályba sorolással, az Információbiztonsági tervvel, valamint a műszaki ellenőr alkalmasságával kapcsolatban benyújtott dokumentumokat, továbbá a Megvalósíthatósági Tanulmányt értékeli és azokkal kapcsolatban szakpolitikai állásfoglalást, a műszaki ellenőr személyével és annak tevékenységével kapcsolatban pedig átiratot bocsát ki. Amennyiben nem ért vele egyet, akkor kiegészítésre, módosításra javasolja a Szakpolitika számára.

⚠ A fent megjelölt dokumentumok elkészítéséhez segítséget jelent a Hatóság honlapján a Hatóság/ DIMOP követelmények menüpontja alatt elérhető sablonok használata.

Az ITB műszaki ellenőr feladatai:

- Konzultáció a projektben érintett szereplőkkel a biztonságtervezés kereteinek meghatározásával kapcsolatban (módszerek, feladatok, ütemezés, felelősségek).
- Az egyes fázisok eredménytermékeihez (előzetes kockázatértékelés és előzetes biztonsági osztályba sorolás, Információbiztonsági terv) tartozó szakvélemények elkészítése, szakmai validálása, valamint a Hatóság részere történő megküldése, tájékoztatás, illetve véleményezés céljából.

II. Tervezési fázis – funkcionális biztonságtervezés:

A Rendszerbiztonsági terv célja, hogy áttekintést nyújtson a fejlesztendő EIR biztonsági követelményeiről és ismertesse az alkalmazott, vagy tervezett védelmi intézkedéseket. A Rendszerbiztonsági terv meghatározza továbbá a rendszerhez hozzáférő valamennyi személy felelősségét és elvárt viselkedését.

A Rendszerbiztonsági terv célja továbbá:

- a megfelelő, költséghatékony védelem kialakításának elősegítése a rendszerek fejlesztési szakaszában, illetve az EIR életciklusának további fázisaiban;
- a biztonsági tevékenységek következetes végrehajtásának és személyi változások esetén történő fenntartásának támogatása;
- a biztonsági követelményeknek való megfelelés támogatása;
- a biztonsági intézkedések minőségbiztosításának támogatása.

A Kedvezményezett feladatai:

- Az NBSZ NKI ajánlása alapján Rendszerbiztonsági tervet kell készíteni.

⚠ **Figyelem! A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 41/2015. (VII. 15.) BM rendeletet 2024.12.31. napjával hatályon kívül helyező MK rendelet alapján a Rendszerbiztonsági terv dokumentum sablon felülvizsgálatra és frissítésre került.**

A 2025.01.01-től alkalmazandó Rendszerbiztonsági terv sablonok alábbi linkeken tölthetők le:

- NBSZ – Rendszerbiztonsági terv sablon_NIS2_Alap V.1.0.
- NBSZ – Rendszerbiztonsági terv sablon_NIS2_Jelentős V.1.0.
- NBSZ – Rendszerbiztonsági terv sablon_NIS2_Magas V.1.0.

A korábbi **(a 2024.12.31-ig indult fejlesztések során használható)** Rendszerbiztonsági terv sablon itt érhető el:

- NBSZ – Rendszerbiztonsagi-terv-sablon.docx

- Az NBSZ NKI ajánlása alapján szükséges kialakítani a projekt keretében létrehozott EIR incidenskezelési módszertanát. A módszertant a Rendszerbiztonsági tervben kell szerepeltetni.
- Az NBSZ NKI-val együttműködve meg kell vizsgálni - és amennyiben a csatlakozás megvalósulásának nincs elháríthatatlan akadálya, akkor **a Rendszerbiztonsági tervben dokumentálni kell - a Kormányzati Elosztott Hálózatbiztonsági Csapdarendszerhez (GovProbe, honeypot) való kapcsolódás szintjének lehetőségeit.**

  A GovProbe rendszerhez történő kapcsolódás részletes paramétereit az NBSZ NKI-val történt egyeztetést követően, az NBSZ NKI által készített dokumentumokból (pl.: Kitelepítési útmutató a befogadó rendszerek részére) ismerhető meg. Az NBSZ NKI által üzemeltetett csapdarendszer egy központi adatgyűjtő, kiértékelő elemből, valamint az azzal kapcsolatban álló, külső támadó számára valósnak látszó hálózati szolgáltatásokat szimuláló, a védendő rendszerbe kihelyezett célpontokból (szenzorok) áll.

  A Kedvezményezett a fejlesztés részeként vállalja, hogy a csatlakozás alapvető műszaki feltételeit a fejlesztés keretében megteremti és azt a rendszer teljes életciklusában fenntartja. A Kedvezményezettnek biztosítania kell a szenzor műszaki/technikai méretezéséhez szükséges adatokat, biztosítani kell a telepítést, a kapcsolódást és egyéb infrastrukturális feltételeket.

- Az NBSZ NKI-val együttműködve meg kell vizsgálni - és amennyiben a csatlakozás megvalósulásának nincs elháríthatatlan akadálya, akkor a Rendszerbiztonsági tervben dokumentálni kell - a Reaktív, IDS típusú eseménydetekciós céllal létrehozott korai megelőző rendszerhez (EWS) való csatlakozás lehetséges módjait (Korai Figyelmeztető Rendszer (EWS)– Szolgáltatási Szabályzat).

  Az EWS rendszer szolgáltatásai javítják a csatlakozó intézmény észlelési, felügyeleti és megfelelőség-ellenőrzési képességét.

  Amennyiben az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) Korm. rendelet alapján a szolgáltatást igénybe veszi, a Kedvezményezett a fejlesztés részeként vállalja, hogy az NBSZ által üzemeltetett EWS-hez való csatlakozás alapvető műszaki feltételeit a fejlesztés keretében megteremti és azt a rendszer teljes életciklusában fenntartja.

  A Kedvezményezett tudomásul veszi, hogy a jelzőrendszer a központosított szolgáltató által nyújtott biztonsági szolgáltatásokat, rendszereket nem érinti, azokat nem váltja ki és nem helyettesíti a Kedvezményezett által létesítendő rendszerelemeket sem, hanem azokat védelmi szempontból kiegészíti, támogatja.

- Az NBSZ NKI-val együttműködve meg kell vizsgálni, és amennyiben a csatlakozás megvalósulásának nincs elháríthatatlan akadálya a Rendszerbiztonsági tervben dokumentálni kell az NBSZ NKI incidenskezelési platformjára történő csatlakozás lehetőségeit.
- Az NBSZ NKI-val együttműködve meg kell vizsgálni és amennyiben a csatlakozás megvalósulásának nincs elháríthatatlan akadálya a Rendszerbiztonsági tervben dokumentálni kell az Automata Sérülékenységvizsgálati Rendszeréhez (ASR) történő csatlakozás lehetséges módjait.

  Az NBSZ NKI által közzétett módon, az adategyezető dokumentum kitöltésével és megküldésével szükséges kezdeményezni a csatlakozást, amennyiben az technológia szempontból lehetséges.

Az ITB műszaki ellenőr feladatai:

- A Rendszerbiztonsági terv készítésének ellenőrzése (folyamat ellenőrzés), a Rendszerbiztonsági terv eredménytermékének szakmai validálása (eredménytermék ellenőrzés), valamint a Rendszerbiztonsági tervvel kapcsolatos szakvélemény készítése és az NBSZ NKI-nak történő megküldése.
- A GovProbe (honeypot), az EWS, az ASR, az incidenskezelési platform rendszerhez való kapcsolódás vizsgálatának (Kedvezményezett végzi a vizsgálatot) ellenőrzése, valamint szakvélemény készítése és az NBSZ NKI-nak történő megküldése.
- Negyedéves, valamint mérföldkövekhez kapcsolódó jelentés elkészítése és a Hatóság részére – tájékoztatás céljából – történő megküldése az információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelmények megvalósulásáról.

⚠ A Hatóság a Rendszerbiztonsági tervet, valamint a GovProbe, az EWS, az ASR, az incidenskezelési platform rendszerrel kapcsolatban elkészített dokumentumokat értékeli. Amennyiben megfelelőnek ítéli meg, a Hatóság jóváhagyja, amennyiben nem ért vele egyet, akkor kiegészítésre, módosításra visszaküldi az ITB műszaki ellenőr, valamint a Kedvezményezett részére.

III. Megvalósítási fázis:

A projekt kivitelezése az Információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelményeknek megfelelően. A megvalósítás során, a tervektől történő eltérések átvezetése a Rendszerbiztonsági tervből a rendszerbiztonsági dokumentumba.

A Kedvezményezett feladatai:

Az NBSZ NKI bevonásával kell elvégezni a sérülékenységvizsgálati tevékenység tervezését. A megvalósítás tervezett módját a Rendszerbiztonsági tervben szükséges bemutatni.

A projekt kivitelezése az Információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelményeknek megfelelően.

A megvalósítás során, a tervektől történő eltérések átvezetése a Rendszerbiztonsági tervből a rendszerbiztonsági dokumentumba.

Az ITB műszaki ellenőr feladatai:

- Az információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelmények megfelelő megvalósulásának ellenőrzése (folyamat, dokumentum és eredménytermék ellenőrzés), a megvalósulás előrehaladásáról, esetleges problémáiról készülő riportok továbbítása az NBSZ NKI és a Kedvezményezett felé tájékoztatásra.
- Negyedéves, valamint mérföldkövekhez kapcsolódó jelentés elkészítése és a Hatóság részére – tájékoztatás céljából – történő megküldése az információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelmények megvalósulásáról.
- A rendszerbiztonsági dokumentummal kapcsolatos szakvélemény elkészítése.

⚠ A Hatóság a Rendszerbiztonsági tervet, a mérföldkövekhez kapcsolódó jelentéseket, valamint a biztonsági követelmények megvalósulásának előrehaladásáról, esetleges problémáiról készülő riportokat értékeli. Amennyiben megfelelőnek ítéli meg, a Hatóság jóváhagyja, amennyiben nem ért vele egyet, akkor kiegészítésre, módosításra visszaküldi az ITB műszaki ellenőr és a Kedvezményezett részére.

IV. Lezárási fázis:

Az Információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelmények maradéktalan megvalósítása a rendszer éles üzemének megkezdését megelőzően.

A Kedvezményezett feladatai:

- Éles üzembe állítást megelőző sérülékenységvizsgálat tervezése, annak megvalósítása az NBSZ NKI bevonásával, valamint az NBSZ NKI sérülékenységvizsgálati jelentésében foglalt sérülékenységek javítása. A sérülékenységvizsgálattal kapcsolatos információk elérhetőek a Hatóság honlapján, az Intézet / Szolgáltatások / Sérülékenységvizsgálat menüpontja alatt.
- Az NBSZ NKI-val együttműködve a CTI (Cyber Threat Intelligence) platformhoz való kapcsolódás lehetőségének vizsgálata.

- CTI (Cyber Threat Intelligence) platformhoz való kapcsolódás esetén legalább 1 fő, a projektben részt vevő szakértő (külső vagy belső) vonatkozásában sikeres CTI képzésen való részvétel.

Az ITB műszaki ellenőr feladatai:

- Az Információbiztonsági tervben, valamint a Rendszerbiztonsági tervben meghatározott biztonsági követelmények végső megvalósulásának ellenőrzése.
- A sérülékenységvizsgálati tevékenység tervének ellenőrzése és a sérülékenységvizsgálati terv véleményezése, a sérülékenységvizsgálati állásfoglalásban feltárt hiányosságok javítására tett intézkedések dokumentációjának ellenőrzése és véleményezése.
- A CTI platformhoz való kapcsolódási dokumentum biztonsági fókuszú ellenőrzése és a kapcsolódási dokumentum véleményezése.
- Javaslattétel a biztonsági követelmények megvalósulásának belső elfogadására.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2025