Elektronikus információbiztonsági követelmények a Nemzeti Kommunikáció Hivatal által működtetett Portálon regisztráló érintett szervezetek számára

Verzió: v1.0; 2026. 04. hó 23. nap

Dokumentum célja

A Nemzeti Kommunikációs Hivatal (a továbbiakban: NKOH), mint – a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (továbbiakban: Kiberbiztonsági tv.) 4. § 60. pontjában meghatározottak szerinti – központi rendszer felett rendelkezési jogot gyakorló kiemelt felelőssége, hogy az általa működtetett Központosított Közbeszerzési Portál (a továbbiakban: Portál) megfelelő védelmi mechanizmusokkal rendelkezzen, ugyanakkor az ezen központi rendszerben regisztrált felhasználó szervezetek kötelessége, hogy a saját belső működésükben és rendszerükben is biztosítsák az NKOH által meghatározott elektronikus információbiztonsági követelményeket a központi rendszer védelme érdekében.

A jelen dokumentumban NKOH - a Kiberbiztonsági tv. 18. § (1) bekezdés c) pontjában foglaltak alapján meghatározza az információbiztonsági követelményeket minden olyan szervezet számára, amely, mint érintett szervezet az NKOH által működtetett Portálon történő regisztrációt követően ezen központi rendszert felhasználó szervezetté válik. A dokumentumban megfogalmazott követelmények biztosítják az adatok védelmét, a központosított közbeszerzési szolgáltatások folyamatos rendelkezésre állását, valamint a Kiberbiztonsági tv.-nek, továbbá a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetén alkalmazandó konkrét védelmi intézkedésekről 7/2024. (VI. 24.) MK rendeletnek és az MSZ ISO/IEC 27001:2023 szabványnak való megfelelést.

Dokumentum hatálya és alkalmazási területe

Az NKOH által meghatározott jelen követelményrendszer minden olyan intézményre, szervezetre és azok természetes személy végfelhasználóira vonatkozik, aki(k) a Nemzeti Kommunikációs Hivatal jogállásáról és a kormányzati kommunikációs beszerzésekről szóló 162/2020. (IV. 30.) Korm. rendelet 1. § (2) bekezdés 3. pontja alapján a regisztráltak a Portálra és érintett szervezetként a Portálhoz hozzáférnek, valamint ennek keretében adatot továbbítanak, fogadnak vagy feldolgoznak (továbbiakban: regisztrált érintett szervezet). Jelen dokumentum érinti az NKOH által működtetett Portál - mint központi rendszer - használatát, valamint az ahhoz kapcsolódó dokumentumok, információk feldolgozását és kezelését.

A jelen dokumentumban meghatározott követelmények kötelező érvényűek, azokat a Portálra való belépéssel a regisztrált érintett szervezet és annak felhasználója elfogadja.

Kötelező felülvizsgálat rendje

Az elektronikus információbiztonsági követelményeket meghatározó jelen dokumentum felülvizsgálata az alábbiak szerint történik:

- évente egy alkalommal, a belső felülvizsgálatok során,
- minden olyan esetben, amikor jelen dokumentumban leírtakhoz képest jelentős változás történik,
- az eredeti szabályozás alapjait érintő minden változás (új kockázatok, új káresemények, új veszélyhelyzetek, és a műszaki infrastruktúra átalakítása) esetén, soron kívül.

A mindenkori felülvizsgálat végrehajtása az információbiztonsági felelős (a továbbiakban: IBF) feladata az NKOH szakterületileg érintett munkatársainak közreműködésével.

Általános kötelezettségek

A regisztrált érintett szervezet az elektronikus információs rendszereinek a nemzeti kiberbiztonsági hatóság részére történő bejelentése során a Portál, mint központi rendszer használatát – a központi rendszer azonosítására alkalmas adatok, valamint a központi rendszer felett rendelkezési jogot gyakorló szervezet (NKOH) megjelölésével – bejelenti. A regisztrált érintett szervezet az NKOH által meghatározott elektronikus információbiztonsági követelményeket teljesíti, valamint – amennyiben azzal rendelkezik – rögzíti azokat az információbiztonsági szabályzatában.

A regisztrált érintett szervezetek felelősek a rendszer rendeltetésszerű használatáért, a rájuk bízott hitelesítő adatok védelméért, valamint az információbiztonsági követelmények betartásáért. NKOH felel a rendszer biztonságos működtetéséért, a központi hozzáférés-kezelésért és a biztonsági események kezelésének koordinálásáért. A regisztrált érintett szervezet és NKOH együttműködik az információbiztonsági kockázatok kezelésében és az incidensek kivizsgálásában.

Szerepkörök és felelősségek

A regisztrált érintett szervezet köteles az NKOH által meghatározott, a Portál használatával összefüggő felelősségi rendet olyan részletességgel rögzíteni, hogy egy információbiztonsági

esemény vagy hozzáférési jogosultság esetén egyértelmű legyen, ki jogosult dönteni, intézkedni és kommunikálni. A szerepkörök kijelölése történhet név szerint vagy szervezeti szerepkör szerint, de mindkét esetben biztosítani kell a helyettesítést.

Adatkezelési, adatvédelmi és információbiztonsági előírások

A Portál használatakor minden felhasználónak be kell tartani az adatkezelési előírásokat.

Az adatkezelési tájékoztató ezen a linken érhető el.

A Portálon csak olyan adatkezelés végezhető, amely a feladat ellátásához feltétlenül szükséges.

A Portált használó regisztrált érintett szervezeteknek gondoskodni kell arról, hogy az adatokhoz való a hozzáférési jogosultságok a legkisebb jogosultság elve mentén kerüljenek kiosztásra.

Az adatok harmadik fél részére történő továbbítására kizárólag jogszabályi kötelezettség teljesítése, illetve a központi rendszer működtetéséhez szükséges adatfeldolgozói jogviszony keretében kerülhet sor.

A tárolt adatokhoz való hozzáférést korlátozni kell és védeni kell az illetéktelen hozzáférésektől.

Biztonságtudatossági képzés

A Portált igénybe vevő regisztrált érintett szervezet gondoskodik arról, hogy a rendszerhez hozzáférő felhasználók a rendszer biztonságos használatához szükséges alapvető információbiztonsági ismeretekkel rendelkezzenek, ennek érdekében általános biztonságtudatossági képzést biztosít a Portál felhasználói számára – beleértve a vezetőket, felsővezetőket és szerződéses partnereket –, az első hozzáférés megadása előtt, majd azt követően a regisztrált érintett szervezet által meghatározott gyakorisággal.

Regisztrációs, hozzáférési és jogosultságkezelési követelmények

A Portálon történő regisztráció előtt a regisztráló érintett szervezetnek gondoskodnia kell a jelen dokumentumban előírt információbiztonsági előírásoknak való megfelelőségről.

A Portálhoz való hozzáférés csak előzetesen regisztrált érintett szervezeteknek engedélyezett, a Portál kizárólag központilag jóváhagyott, a regisztrált érintett szervezethez kapcsolódó szervezeti azonosítóval érhető el.

A Portálon regisztrált érintett szervezet köteles minden szükséges adatot megadni a szervezeti és felhasználói hozzáférés elkészítéséhez. A felhasználó a rendszerben hozza létre a jelszavát. A szervezeti felhasználói fiók létrehozásához szükséges személyes adatok:

- Vezetéknév
- Keresztnév
- Email
- Telefonszám

A Portálon használt hitelesítő eszközöknek - jelszavaknak meg kell felelniük a központi rendszer üzemeltető által előírt jelszókövetelményeknek.

Fájlkezelés, nyomtatás és adathordozók kezelése

A Portálról letöltött vagy exportált adatok kezelése során a regisztrált érintett szervezet köteles a másolatkészítést minimalizálni, valamint biztosítani, hogy az adatok ne kerüljenek illetéktelen személy birtokába elektronikus vagy papíralapú formában.

Amennyiben a regisztrált érintett szervezet adathordozót alkalmaz, javasolt nyilvántartást vezetni az adathordozó kiadásáról, tartalmáról, tárolásáról és visszavételéről.

Távoli munkavégzés és mobil hozzáférés követelményei

A Portál távoli munkavégzés során történő használata akkor engedélyezett, ha a regisztrált érintett szervezet biztosítja az eszköz és a hozzáférés megfelelő védelmét, valamint a környezetből eredő kockázatok kezelését. Távoli munkavégzés alatt értendő különösen az otthoni munkavégzés, utazás közbeni munkavégzés, illetve bármely olyan helyzet, amikor a felhasználó nem a regisztrált érintett szervezet ellenőrzött telephelyén végzi feladatait.

Biztonságos böngésző- és munkakörnyezet beállítások

A Portál használata elsősorban korszerű és támogatott böngészőkkel engedélyezett. A regisztrált érintett szervezet köteles biztosítani, hogy a felhasználók által alkalmazott böngészők és bővítmények ne csökkentsék a biztonságot, továbbá ne okozzanak információbiztonsági és adatvédelmi kockázatot.

E-mail és elektronikus kommunikáció biztonsága

A Portálról származó adatok e-mailben történő továbbítása kockázatot jelenthet, ezért a regisztrált érintett szervezet köteles az ilyen jellegű továbbításokat szabályozni és indokolt esetben korlátozni. A harmadik fél részére történő adattovábbítást csak engedélyezett és megfelelően kontrollált körülmények között köteles megvalósítani.

Adatmegőrzés, archiválás és biztonságos törlés

A regisztrált érintett szervezet köteles a Portálról származó adatok megőrzését és törlését olyan módon szabályozni, hogy az megfeleljen a vonatkozó jogszabályi és belső előírásoknak, valamint az adatminimalizálás elvének. Az adatok törlését úgy kell végrehajtani, hogy azok utólag ne legyenek visszaállíthatók.

Hálózatbiztonsági követelmények

A regisztrált érintett szervezetek kötelesek a saját hálózati infrastruktúráját úgy kialakítani, hogy az ne veszélyeztesse a központi rendszert. A hálózati kapcsolat minőségéért és stabilitásáért a regisztrált érintett szervezet felel. A nyilvános, nem ismert vagy nem megbízható hálózatokon keresztüli hozzáférés szigorúan tilos. A nem biztonságos kapcsolatok kialakítása vagy fenntartása tilos.

Végpontbiztonság

A Portál biztonságos működésének alapfeltétele a végpontok (munkaállomás, laptop) biztonságos működésének biztosítása különösen naprakész operációs rendszerrel és kártékony

kód elleni védelemmel. A Portál használata nem támogatott, elavult vagy ismeretlen állapotú eszközök használatával nem engedélyezett.

Incidenskezelés

Kiberbiztonsági incidensnek minősül az olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát.

Gyanús vagy szokatlan felhasználói tevékenységeket a regisztrált érintett szervezet információbiztonsági, vagy adatvédelmi felelőse köteles haladéktalanul kivizsgálni és szükség esetén bejelenteni NKOH részére.

A regisztrált érintett szervezeteknek az NKOH-t érintő incidenseket haladéktalanul, de legkésőbb 24 órán belül jelenteni kell NKOH részére. Az incidensjelentést elektronikus úton kell megtenni a dpo@nkoh.gov.hu, valamint az ibf@nkoh.gov.hu e-mail címre küldött levél formájában.

Fizikai biztonsági előírások

A fizikai biztonság célja, hogy megakadályozza a jogosulatlan hozzáférést, az adatok illetéktelen megismerését, károkozást és az eszközök sérülését.

A Portálon regisztrált érintett szervezetnek gondoskodni kell, hogy a Portálhoz való hozzáférés kizárólag az arra jogosult felhasználók számára legyen biztosított, ami során a felhasználók olyan ellenőrzött fizikai környezetben járjanak el, amely nem teszi lehetővé illetéktelen személyek számára a Portál adatainak megismerését.

Kivételkezelés és kockázatvállalás rendje

Előfordulhat, hogy a regisztrált érintett szervezet bizonyos követelmények teljesítését átmenetileg nem tudja biztosítani. Ilyen esetben a regisztrált érintett szervezet köteles kockázatértékelést végezni és dokumentálni. Jelen követelményektől való eltérés kizárólag indokolt esetben, dokumentált módon és a kockázatok mérlegelését követően lehetséges.

Védelmi intézkedések igazolása és dokumentálás

A regisztrált érintett szervezet köteles a Portál használatához kapcsolódó védelmi intézkedések meglétét belsőleg dokumentálni, és NKOH kérésére azt igazolni. Az igazolás célja nem a regisztrált érintett szervezet működésének indokolatlan terhelése, hanem a központi rendszer információbiztonságának, védelmének fenntartása.

Ellenőrzési jogosultság

NKOH fenntartja a jogot, hogy indokolt esetben és mértékben ellenőrzést tartson a Portált használó regisztrált érintett szervezeteknél a Portál biztonságos használatával összefüggő feladatok végrehajtásának ellenőrzése érdekében.

Soron kívüli ellenőrzést NKOH csak incidens, biztonsági kockázat vagy szabálysértés gyanúja esetén tart. Az ilyen ellenőrzés során a Portált használó regisztrált érintett szervezetek kötelesek haladéktalanul együttműködni.

Szankciók és felelősségek

NKOH a jelen dokumentumban leírt követelmények be nem tartása esetén az ellenőrzés során feltárt hiányosságok pótlására, hibák javítására határidő jelölésével felszólítja a felhasználó szervezetet, ennek eredménytelensége esetén további intézkedések megtétele érdekében tájékoztatja a nemzeti kiberbiztonsági hatóságot.

A jelen dokumentumban foglalt kötelezettségek súlyos megszegése esetén NKOH jogosult a polgári jog általános szabályai szerint jogi eljárást kezdeményezni és kártérítési igénnyel is élhet. A Portál rendeltetésszerű használata alapkövetelmény, a nem rendeltetésszerű használattal okozott kárért a regisztrált érintett szervezet a polgári jog szabályai szerint köteles helytállni.

A Portálon regisztrált érintett szervezeteknek, azok természetes személy felhasználóinak kötelező a rendszerhasználati feltételek, szabályok ismerete és betartása.

Mellékletek

Melléklet 1 - Incidensbejelentő sablon (minimum tartalom)

Az alábbi minta a bejelentés minimális tartalmi elemeit tartalmazza. A bejelentés célja, hogy NKOH gyorsan be tudja azonosítani az eseményt és meghatározza a szükséges intézkedéseket.

- Bejelentő szervezet neve:
- Kapcsolattartó neve és elérhetősége (telefon, e-mail):
- Esemény észlelésének időpontja:
- Esemény feltételezett kezdete (ha ismert):
- Regisztrált érintett szervezet felhasználói azonosítója (ha ismert):
- Érintett eszköz(ök) típusa és azonosítója (ha rendelkezésre áll):
- Rövid leírás: mi történt, milyen tünetek voltak és hogyan derült ki:
- Érintett adatok jellege (ha ismert):
- Azonnali és tervezett intézkedések: milyen lépések történtek és esedékesek a károk csökkentésére:
- Bizonyítékok: napló, riasztás, képernyőkép rendelkezésre áll-e:
- Feltételezett vagy bekövetkezett kárhatás: működéskiesés, adatszivárgás gyanúja, visszaélés gyanúja:
- Jövőbeli tervezett intézkedések a hasonló incidensek elkerülése céljából.