Slachta Margit
Nemzeti Szociálpolitikai
Intézet

Információbiztonsági követelmények a PKR rendszert igénybe vevő felhasználó szervezetek számára

Jelen követelményrendszer célja az adatok védelmének, a szolgáltatások folyamatos rendelkezésre állásának, valamint a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvénynek, a 7/2024. (VI. 24.) MK rendeletnek való megfelelés biztosítása. A szabályok kötelező érvényűek minden olyan szervezetre, amely az PKR rendszerhez hozzáfér, adatot továbbít, fogad vagy feldolgoz.

Jelen követelményrendszer minden olyan intézményre, szervezetre (továbbiakban: felhasználó szervezet) és azok természetes személy végfelhasználóira vonatkozik, aki(k) regisztráltak az PKR rendszerben és ahhoz hozzáférnek, valamint ennek keretében adatot továbbítanak, fogadnak vagy feldolgoznak.

A jelen dokumentumban meghatározott követelmények kötelező érvényűek, azokat a PKR rendszerbe való belépéssel a felhasználó szervezet és annak felhasználója elfogadja.

1. Általános megfelelés és bejelentés

- A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (továbbiakban: Kiberbiztonsági tv.) hatálya alá tartozó felhasználó szervezet köteles az elektronikus információs rendszereinek a nemzeti kiberbiztonsági hatóság részére történő bejelentése során az PKR rendszer használatát – a rendszer azonosítására alkalmas adatok, valamint a rendszer felett rendelkezési jogot gyakorló szervezet (NSZI) megjelölésével – bejelenteni.
- A felhasználó szervezet köteles a jelen dokumentumban meghatározott elektronikus információbiztonsági követelményeket teljesíteni, valamint – amennyiben azzal rendelkezik – azokat az információbiztonsági szabályzatában rögzíteni.
- A PKR rendszerben történő regisztráció előtt a felhasználó szervezetnek gondoskodnia kell a jelen dokumentumban előírt információbiztonsági előírásoknak való megfelelőségről.

2. Szerepkörök és felelősségek

- A felhasználó szervezet köteles felelősséget vállalni a rendeltetésszerű használatért, a hitelesítő adatok védelméért és az incidensek kivizsgálásában való együttműködésért.
- A felhasználó szervezet köteles kijelöli azokat a személyeket, akik jogosultak a rendszer használatára, és felelősek a hozzáférések igényléséért, módosításáért és megszüntetéséért.
- A felhasználók felelősek a rendszer rendeltetésszerű használatáért, a rájuk bízott hitelesítő
  adatok védelméért, valamint az információbiztonsági követelmények betartásáért.
- A felhasználó szervezet köteles együttműködni az információbiztonsági kockázatok kezelésében és az incidensek kivizsgálásában.
- A felhasználó szervezet köteles biztosítani, hogy a rendszerhez hozzáférő felhasználók alapvető információbiztonsági tudatossággal rendelkezzenek, különös tekintettel az adatok bizalmas kezelésére, a jogosulatlan hozzáférések megelőzésére és az incidensek felismerésére.

3. Hozzáférés és jogosultságkezelés

- A felhasználók kizárólag a munkakörük ellátásához szükséges jogosultságokat kaphatják meg, és kötelesek gondoskodni hitelesítő adataik bizalmas kezeléséről.

4. Adatkezelés és adatbiztonság

- A rendszerből letöltött, exportált vegy egyéb módon kinyert adatok kezelése során biztosítani kell azok jogosulatlan hozzáféréstől való védelmét. Az adatok nyomtatása és külső adathordozóra mentése csak indokolt esetben, a szervezet belső szabályainak megfelelően történhet.
- A rendszerből származó információk elektronikus továbbítása során biztosítani kell, hogy azok kizárólag jogosult címzettekhez kerüljenek. Bizalmas adatokat tartalmazó információk nyilvános vagy nem védett csatornán történő továbbítása nem megengedett.
- A rendszerből származó adatok megőrzése kizárólag a jogszabályi vagy működési kötelezettségek által indokolt ideig történhet. Az adatok törlését oly módon kell végrehajtani, hogy azok utólag ne legyenek visszaállíthatók.
- Az adatok harmadik fél részére történő továbbítására kizárólag jogszabályi kötelezettség teljesítése, illetve a rendszer működtetéséhez szükséges adatfeldolgozói jogviszony keretében kerülhet sor.
- Az PKR rendszerben csak olyan adatkezelés végezhető, amely a feladat ellátásához feltétlenül szükséges.

5. Technikai védelem és környezeti biztonság

- A rendszer elérése naprakész, gyártó által támogatott böngészőből történhet. A felhasználók kötelesek olyan munkakörnyezetet használni, amely védett a jogosulatlan hozzáféréstől.
- A rendszerhez történő hozzáférés során a felhasználó szervezet köteles biztosítani, hogy a hálózati környezet védett legyen a jogosulatlan hozzáférésekkel és ismert támadásokkal szemben.
- A rendszerhez hozzáférő végpontoknak (pl. munkaállomás, laptop) rendelkezniük kell alapvető védelmi intézkedésekkel, különösen naprakész operációs rendszerrel és kártékony kód elleni védelemmel.
- A rendszerhez hozzáférő eszközöket olyan környezetben kell használni, amely megakadályozza a jogosulatlan fizikai hozzáférést és az adatok illetéktelen megismerését.
- Nyilvános vagy nem megbízható hálózatokon keresztül a rendszerhez történő hozzáférés tilos.

6. Incidenskezelés, ellenőrzés, szankciók

- A felhasználó szervezet az PKR rendszert érintő, általa észlelt, Kiberbiztonsági tv. szerinti kiberbiztonsági incidenseket köteles bejelenteni az NSZI részére az infosec@nszi.gov.hu e-mail címen. (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.)
- A jelen követelményektől való eltérés kizárólag indokolt esetben, dokumentált módon és a kockázatok mérlegelését követően engedélyezhető.

- A felhasználó szervezet kérésre köteles igazolni, hogy a jelen dokumentumban meghatározott alapvető információbiztonsági követelményeket alkalmazza.
- Az NSZI fenntartja a jogot, hogy indokolt esetben és mértékben ellenőrzést tartson az PKR rendszert használó szervezeteknél a rendszer biztonságos használatával összefüggő feladatok végrehajtásának ellenőrzése érdekében. Soron kívüli ellenőrzést az NSZI csak incidens, biztonsági kockázat vagy szabálysértés gyanúja esetén tart. Az ilyen ellenőrzés során a Portált használó regisztrált érintett szervezetek kötelesek haladéktalanul együttműködni.
- Az NSZI 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 az NSZI jogosult a polgári jog általános szabályai szerint jogi eljárást kezdeményezni és kártérítési igénnyel is élhet. Az PKR rendszer rendeltetésszerű használata alapkövetelmény, a nem rendeltetésszerű használattal okozott kárért a regisztrált érintett szervezet a polgári jog szabályai szerint köteles helytállni.