Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Személyi biztonság

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

14.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

14.1. A szervezet:

14.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint

14.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó személyi biztonságra vonatkozó szabályzatot, amely

14.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá

14.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

14.1.1.2. A személyi biztonságra vonatkozó eljárásrendet, amely a személyi biztonságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

14.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a személyi biztonságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

14.1.3. Felülvizsgálja és frissíti az aktuális személyi biztonságra vonatkozó szabályzatot és a személyi biztonságra vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A személyi biztonságra vonatkozó szabályzatnak és a kapcsolódó eljárásrend(ek)nek illeszkednie kell az érintett szervezet kockázatkezelési stratégiájához. A megfelelő minőségben és megfelelő szempontok mentén elkészített szabályzatok és eljárásrendek nagy mértékben járulnak hozzá a szervezet biztonságának megőrzéséhez. Az elkészült szabályzatoknak és eljárásrendeknek összhangban kell lenniük egymással és a szervezet információbiztonsági környezetével. A szervezeti szintű biztonsági szabályzatok és eljárásrendek használata általában előnyösebb, hiszen szükségtelenné teheti a különböző szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. A szervezet azonban dönthet úgy (amennyiben a szervezet felépítése ezt indokolja), hogy a szabályzati szinten megjelenő követelményeket egy általános biztonsági szabályzatban [pl.: Információbiztonsági Szabályzat (IBSZ)], vagy

több szabályzatban implementálja, míg az eljárásrendek szintjén megjelenő követelményeket (melyek a szabályzatban foglalt követelményeket részletezik rendszer- és szerepköri szinten) beépítheti a rendszerbiztonsági tervébe, vagy több különböző dokumentumban jeleníti meg azokat. A szervezetnek kiemelt figyelmet kell fordítania mind a szabályzat, mind az eljárásrendek megfelelő frissítésére. A frissítéseket kiváltó események lehetnek értékelésből vagy (felül)vizsgálatból eredő megállapítások, biztonsági események vagy változások a hatályos jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. A szervezetnek szem előtt kell tartania, hogy az elvárt védelmi intézkedések egyszerű újraközlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a személyi biztonságra vonatkozó szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a személyi biztonságra vonatkozó szabályzatban foglaltak megfelelnek a szervezetre vonatkozó hatályos jogszabályoknak, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak.
3. A szervezetnek - a megfelelő szereplők bevonásával, dokumentált módon - ki kell dolgoznia a vonatkozó szabályzatot és a kapcsolódó eljárásrendeket, és gondoskodnia kell a szabályzat és az eljárásrendek megfelelő kihirdetéséről, valamint az érintett felekkel történő megismertetéséről.
4. A szabályzat és a kapcsolódó eljárásrendek kidolgozásánál a szervezetnek figyelembe kell vennie a rá vonatkozó sajátosságokat. Az elvárt védelmi intézkedések szó szerinti átvétele nem minősül szervezeti szabályzatnak vagy eljárásrendnek.
5. A szervezetnek a gyakorlatban is alkalmaznia kell a személyi biztonságra vonatkozó szabályzatban és az ahhoz kapcsolódó eljárásrendekben megfogalmazott elvárásokat, ezáltal biztosítva azok tényleges megvalósulását.
6. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell az aktuális személyi biztonságra vonatkozó szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

Kapcsolódó intézkedések

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

5.2; 5.3; 7.5.1; 7.5.2; 7.5.3; A.5.1; A.5.2; A.5.4; A.5.31; A.5.36; A.5.37

NIST SP 800-53 rev.5 referencia

PS-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

14.2. MUNKAKÖRÖK BIZTONSÁGI SZEMPONTÚ BESOROLÁSA

14.2. A szervezet:

14.2.1. minden szervezeti munkakörhöz hozzárendel egy kockázati besorolást;

14.2.2. átvilágítási kritériumokat állít fel a munkaköröket betöltő egyének számára; és

14.2.3. meghatározott gyakorisággal felülvizsgálja és frissíti a kockázati besorolást.

MAGYARÁZAT

Az érintett szervezet minden munkakörhöz hozzárendel egy kockázati besorolást. Értékeli egy pozíció feladatait és felelősségeit annak meghatározására, hogy a pozíció betöltőjének hibázása esetén milyen mértékben okozhat kárt a szolgáltatás hatékonyságában vagy sértetlenségében, amely alapján meghatározza a pozíció kockázati szintjét. Az értékelés azt is meghatározhatja, hogy adott pozíció feladatai és felelősségei milyen mértékben lehetnek károsak anyagilag vagy gyakorolhatnak negatív hatást a nemzetbiztonságra, és ennek a potenciális hatásnak a mértékét. Az értékelés eredményei meghatározzák, hogy milyen szintű átvilágítás történik egy pozícióra nézve. A kockázati besorolások iránymutatást adhatnak és informatívak lehetnek arra nézve is, hogy az adott személynek mekkora mértékű és milyen típusú engedélye van az EIR-hez való hozzáféréshez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek minden szervezeti munkakörhöz hozzá kell rendelnie egy kockázati besorolást.

2. A szervezetnek létre kell hoznia egy besorolási rendszert a munkakörökhöz, amely értékeli a pozíció feladatait és felelősségeit.

3. A szervezetnek átvilágítási kritériumokat kell felállítania a munkaköröket betöltő személyek számára.

4. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie a kockázati besorolást.

Kapcsolódó intézkedések

2.59. Felelősségek szétválasztása

3.9. Szerepkör alapú biztonsági képzés

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

13.2. Rendszerbiztonsági terv

14.3. Személyek háttérellenőrzése

14.9. Hozzáférési megállapodások

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

16.98. Külső fejlesztők háttérellenőrzése

18.67. Információ kezelése és megőrzése

41/2015. (VII. 15.) BM rendeleti referencia

3.1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PS-2

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

14.3. SZEMÉLYEK HÁTTÉRELLENŐRZÉSE

14.3. A szervezet:

14.3.1. ellenőrzi az egyéneket, mielőtt engedélyezné a hozzáférésüket a rendszerhez; és

14.3.2. ismételten ellenőrzi az egyéneket a meghatározott feltételeknek megfelelően, ha változás történt az egyén jogosultsági szintjében vagy munkakörében, illetve meghatározott gyakorisággal.

MAGYARÁZAT

Az érintett szervezet ellenőrzi az egyéneket, mielőtt engedélyezné a hozzáférésüket az EIR-hez, és ismételten ellenőrzi az egyéneket a meghatározott feltételeknek megfelelően, ha változás történt az egyén jogosultságában vagy munkakörében, illetve meghatározott gyakorisággal. Az ellenőrzés és az ismételt ellenőrzés célja, hogy biztosítsa az EIR bizalmasságát és sértetlenségét, valamint megvédje az érintett szervezet információit a nem megfelelő hozzáféréstől vagy használattól.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a személyzet ellenőrzésének és ismételt ellenőrzésének szabályait. Az ellenőrzés például háttérkutatásokat és szervezeti ellenőrzéseket is magában foglalhat.

2. A szervezetnek meg kell határoznia a különböző típusú ismételt ellenőrzési feltételeket és gyakoriságokat az EIR-hez hozzáféréssel rendelkező személyek számára.

4. A szervezetnek ellenőriznie kell a személyeket, mielőtt engedélyezné a hozzáférésüket az EIR-hez.

5. A szervezetnek ismételten ellenőriznie kell az egyéneket a meghatározott körülmények bekövetkezése esetén, ha változás történt a személy jogosultsági szintjében vagy munkakörében, illetve meghatározott gyakorisággal.

6. A szervezetnek dokumentálnia kell az ellenőrzésekről és az ismételt ellenőrzésekről, hogy bizonyítékot szolgáltasson a folyamatok megfelelőségéről és a kiberbiztonsági követelmények betartásáról.

Kapcsolódó intézkedések

2.2. Fiókkezelés

8.14. Azonosító kezelés

10.18. Karbantartó személyek

12.2. A fizikai belépési engedélyek

1.13. Belső fenyegetés elleni program

14.2. Munkakörök biztonsági szempontú besorolása

14.9. Hozzáférési megállapodások

14.11. Külső személyekhez kapcsolódó biztonsági követelmények

16.98. Külső fejlesztők háttérellenőrzése

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.6.1

NIST SP 800-53 rev.5 referencia

PS-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

14.4. Személyek háttérellenőrzése – különleges védelmi intézkedéseket igénylő információk

14.4. A szervezet ellenőrzi, hogy azok az egyének, akik hozzáférnek egy speciális védelmet igénylő információkat feldolgozó, tároló vagy továbbító rendszerhez

14.4.1. rendelkeznek-e érvényes hozzáférési engedéllyel; és

14.4.2. esetükben teljesülnek-e a szervezet által meghatározott további személyzeti ellenőrzési kritériumok.

Magyarázat

Az érintett szervezet ellenőrzi, hogy azok az egyének, akik hozzáférnek az EIR-hez, rendelkeznek-e érvényes hozzáférési engedéllyel. Ez azt jelenti, hogy a szervezetnek biztosítania kell, hogy csak azok az egyének férjenek hozzá az EIR-hez, akiknek van jogosultságuk erre. Ez magában foglalja az ellenőrzést, hogy az egyén rendelkezik-e a megfelelő hozzáférési jogosultságokkal, és hogy ezek a jogosultságok még mindig érvényesek-e.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely információk igényelnek speciális védelmet az EIR-en belül.
2. A szervezetnek létre kell hoznia egy hozzáférés engedélyezési rendszert, amely ellenőrzi, hogy az egyének, akik hozzáférnek az EIR-hez, rendelkeznek-e érvényes hozzáférési engedéllyel. Ez magában foglalhatja a felhasználói nevek és jelszavak, biometrikus azonosítók vagy más hitelesítési módszerek használatát.
3. A szervezetnek meg kell határoznia az ellenőrzési kritériumokat. Ez magában foglalhatja a pozíció érzékenységének, a háttérellenőrzési követelményeknek, és más releváns tényezőknek a figyelembe vételét.
4. A szervezetnek rendszeresen dokumentálnia és ellenőriznie kell a hozzáférési engedélyeket és a személyzeti ellenőrzési kritériumokat, hogy biztosítsa, hogy csak azok az egyének férhetnek hozzá az EIR-hez, akik még rendelkeznek az érvényes hozzáférési engedéllyel és megfelelnek a személyzeti ellenőrzési kritériumoknak.

5. Ha a szervezet bármilyen szabálytalanságot észlel, azonnal cselekednie kell, hogy megvédje az EIR-t, beleértve a hozzáférési engedélyek visszavonását, a jelszavak megváltoztatását, vagy más megfelelő intézkedések megtételét.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PS-3(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

14.5. SZEMÉLYEK MUNKAVISZONYÁNAK MEGSZŰNÉSE

14.5. A szervezet az egyéni munkaviszony megszűnésekor:

14.5.1. Meghatározott időn belül letiltja a rendszerhez való hozzáférést.

14.5.2. Megszünteti vagy visszavonja az adott személyhez kapcsolódó összes hitelesítő eszközt és jogosultságot.

14.5.3. Lefolytatja a kilépési interjúkat, amelyek meghatározott információbiztonsági témákat tartalmaznak.

14.5.4. Visszaveszi az összes biztonsági szempontból releváns szervezeti EIR-hez kapcsolódó biztonsági eszközöket.

14.5.5. Fenntartja a hozzáférést a megszűnt munkaviszonyú személy által ellenőrzött szervezeti információkhoz és rendszerekhez.

MAGYARÁZAT

A szervezet tulajdona magában foglalja a hardveres hitelesítési tokeneket, a műszaki kézikönyveket, a kulcsokat, a belépő- és azonosító kártyákat. A kilépő interjúk biztosítják, hogy az elbocsátott személyek megértsék a rájuk vonatkozó és továbbiakban is érvényben lévő információbiztonsági kötelezettségeket, valamint, hogy a megfelelő elszámoltathatóság valósuljon meg a visszaadott szervezeti eszközökkel kapcsolatban. A kilépő interjúk témái közé kell tartozzon, hogy a távozó kollégát emlékeztessék a titoktartási megállapodásokra és a jövőbeli foglalkoztatás lehetséges korlátaira.

Előfordulhat, hogy egyes személyek esetében nem mindig lehetséges a kilépő interjú végrehajtása, ideértve a nem elérhető, vagy beteg kollégákat. A felmondási folyamat lépéseinek időben történő végrehajtása kiemelt fontosságú azon személyek esetében, akik magas jogosultsággal rendelkeztek, illetve akik esetében indokolt az azonnali felmondás. Bizonyos esetekben az is előfordulhat, hogy a rendszerfiókok letiltása is szükséges még azelőtt, hogy a elbocsátott egyént értesítették volna róla.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meghatározott időn belül le kell tiltania annak a személynek az EIR-hez való hozzáférését, akinek munkaviszonya megszűnt.
2. A szervezetnek meg kell szüntetnie vagy vissza kell vonnia az adott személyhez kapcsolódó összes jogosultságot, a munkaviszonyának megszűnésével a távozó személynek pedig minden birtokában álló hitelesítő eszközt.
3. A szervezetnek le kell folytatnia a kilépési interjúkat, amelyek meghatározott információbiztonsági témákat tartalmaznak.
4. A szervezetnek vissza kell vennie az összes biztonsági szempontból releváns, az EIR-hez kapcsolódó biztonsági eszközt.
5. A szervezetnek meghatározott ideig meg kell őriznie a megszűnt munkaviszonyú személy hozzáférését és az általa kezelt információt.
6. A szervezetnek dokumentálnia kell a fenti lépések végrehajtásáról, hogy bizonyíthassa a megfelelő eljárások betartását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

8.14. Azonosító kezelés

12.2. A fizikai belépési engedélyek

1.13. Belső fenyegetés elleni program

14.9. Hozzáférési megállapodások

14.11. Külső személyekhez kapcsolódó biztonsági követelmények

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

3.1.6.4 Eljárás a jogviszony megszűnésekor

ISO/IEC 27001:2023 REFERENCIA

A.5.11; A.6.5

NIST SP 800-53 REV.5 REFERENCIA

PS-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

14.6. Személyek munkaviszonyának megszűnése – Munkaviszony megszűnését követő követelmények

14.6. A szervezet:

14.6.1. Tájékoztatja az elbocsátott munkavállalókat a jogilag kötelező, munkaviszony megszüntetése után érvényes követelményekről, amelyek a szervezeti információk védelmére vonatkoznak.

14.6.2. A munkaviszony megszüntetésének folyamatában megköveteli, hogy az elbocsátott munkavállalók aláírjanak egy nyilatkozatot a munkaviszony megszüntetése utáni követelmények tudomásulvételéről.

Magyarázat

A munkaviszony megszüntetésének folyamatában az érintett szervezet megköveteli azt, hogy az elbocsátott munkavállalók aláírjanak egy nyilatkozatot a munkaviszony megszüntetése utáni követelmények tudomásulvételéről.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell fontolnia, hogy konzultáljon a jogi szakértővel a munkaviszony megszüntetése utáni követelményekkel kapcsolatos kérdésekben.
2. A szervezetnek tájékoztatnia kell a távozó munkavállalókat a munkaviszony megszűnését követő, jogilag is kikényszeríthető kötelezettségeikről és rájuk vonatkozó követelményekről.
3. A szervezetnek biztosítania kell, hogy a távozó munkavállalók megértsék ezeket a követelményeket, és tudják, milyen következményekkel járhat, ha nem tartják be őket.
4. A szervezetnek meg kell követelnie, hogy az elbocsátott munkavállalók aláírjanak egy nyilatkozatot a munkaviszony megszüntetése utáni követelmények tudomásulvételéről és betartásáról.
5. A szervezetnek gondoskodnia kell arról, hogy ezek a nyilatkozatok biztonságosan tárolva legyenek, és hozzáférhetőek legyenek, amennyiben az szükséges.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell ezeket a követelményeket, hogy biztosítsa azok relevanciáját és hatékonyságát az EIR és a szervezeti információ védelme érdekében.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PS-4(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

14.7. SZEMÉLYEK MUNKAVISZONYÁNAK MEGSZŰNÉSE – AUTOMATIZÁLT INTÉZKEDÉSEK

14.7. A szervezet meghatározott automatizált mechanizmusokat alkalmaz annak érdekében, hogy értesítse a meghatározott személyeket vagy szerepköröket az egyén kilépésével összefüggő tevékenységekről, illetve, hogy megszüntesse a hozzáférést a rendszer erőforrásaihoz.

MAGYARÁZAT

Automatizált mechanizmusokat lehet alkalmazni annak érdekében, hogy automatikus riasztásokat vagy értesítéseket küldjenek az érintett szervezet meghatározott személyeinek vagy szerepköreinek, amikor az egyének kilépnek. Az ilyen automatikus riasztásokat vagy értesítéseket számos módon lehet továbbítani, beleértve telefonon, elektronikus levélben, szöveges üzenetben vagy weboldalakon keresztül. Automatizált mechanizmusokat is lehet alkalmazni annak érdekében, hogy gyorsan és alaposan megszüntessék a hozzáférést az EIR erőforrásaihoz, miután egy alkalmazott kilép. A naplózás segíthet az ilyen tevékenységek nyomon követésében és ellenőrzésében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek automatizált mechanizmusokat kell bevezetnie, amelyek képesek automatikus riasztásokat vagy értesítéseket küldeni a szervezet meghatározott személyeinek vagy szerepköreinek, amikor egyének kilépnek.
2. A szervezetnek biztosítania kell, hogy ezek az automatikus riasztások vagy értesítések időben eljussanak a megfelelő személyekhez vagy szerepkörökhöz.
3. A szervezetnek automatizált mechanizmusokat kell alkalmaznia, amelyek képesek gyorsan és alaposan megszüntetni a hozzáférést az EIR erőforrásaihoz, miután egy egyén kilépett.
4. A szervezetnek naplóznia kell az automatizált mechanizmusok által végzett tevékenységeket, beleértve az értesítések küldését és a hozzáférés megszüntetését.
5. A szervezetnek rendszeresen ellenőriznie kell az automatizált mechanizmusok működését, hogy biztosítsa azok hatékonyságát és megbízhatóságát.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PS-4(2)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok illetve a személyek vagy szerepkörök meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

14.8. AZ ÁTHELYEZÉSEK, ÁTIRÁNYÍTÁSOK ÉS KIRENDELÉSEK KEZELÉSE

14.8. A szervezet:

14.8.1. A folyamatos működés követelményeivel összhangban felülvizsgálja és megerősíti a rendszerekhez és létesítményekhez rendelt érvényes logikai és fizikai hozzáférési jogosultságokat minden olyan esetben, amikor az egyének a szervezeten belül más munkakörbe kerülnek áthelyezésre vagy átirányításra.

14.8.2. Meghatározott időn belül kezdeményezi az áthelyezési és átirányítási intézkedéseket.

14.8.3. Szükség szerint módosítja a hozzáférési jogosultságot, hogy az megfeleljen az áthelyezés vagy átirányítás miatt bekövetkező változások működési szükségleteinek.

14.8.4. Meghatározott időn belül értesíti a megadott személyeket vagy szerepköröket.

MAGYARÁZAT

Indokoltnak tekinthető egy áthelyezés, ha a személyzet egy tagja olyan hosszú időre kerül kiküldetésre vagy folyamatosan kiküldésre kerül. Az érintett szervezetek meghatározzák a megfelelő intézkedéseket az áthelyezések vagy átirányítások típusaihoz, legyenek azok állandóak vagy hosszú távúak. Az áthelyezés vagy átirányítás során szükséges tevékenységek közé tartozhatnak a régi kulcsok visszaadása és új kulcsok kiadása, azonosító kártyák és belépőkártyák cseréje; felhasználói fiók bezárása és új fiók létrehozása; a hozzáférési jogosultságok módosítása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek folyamatosan felül kell vizsgálnia és meg kell erősítenie az EIR-hez és létesítményekhez rendelt érvényes logikai és fizikai hozzáférési jogosultságokat. Ez minden olyan esetben szükséges, amikor az egyének a szervezeten belül más munkakörbe, áthelyezésre vagy átirányításra kerülnek.

2. A szervezetnek meghatározott időn belül kezdeményeznie kell az áthelyezési és átirányítási intézkedéseket.

3. A szervezetnek szükség szerint módosítania kell a hozzáférési jogosultságot, hogy az megfeleljen az áthelyezés vagy átirányítás miatt bekövetkező változások működési szükségleteinek.
4. A szervezetnek meghatározott időn belül értesítenie kell a megadott személyeket vagy szerepköröket.

Kapcsolódó intézkedések

2.2. Fiókkezelés
8.14. Azonosító kezelés
12.2. A fizikai belépési engedélyek
1.13. Belső fenyegetés elleni program
14.5. Személyek munkaviszonyának megszűnése
14.11. Külső személyekhez kapcsolódó biztonsági követelmények

41/2015. (VII. 15.) BM rendeleti referencia

3.1.6.5 Az áthelyezések, átirányítások és kirendelések kezelése

ISO/IEC 27001:2023 referencia

A.5.11; A.6.5

NIST SP 800-53 rev.5 referencia

PS-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

14.9. HOZZÁFÉRÉSI MEGÁLLAPODÁSOK

14.9. A szervezet:

14.9.1. Kidolgozza és dokumentálja a szervezeti EIR-ekhez való hozzáférés szabályait.

14.9.2. A szervezet által meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférési szabályokat.

14.9.3. Ellenőrzi, hogy a szervezeti információkhoz és rendszerekhez hozzáférést igénylő személyek

14.9.3.1. a hozzáférés megadása előtt megismerték és dokumentált módon elfogadták a vonatkozó hozzáférési szabályokat; és

14.9.3.2. a hozzáférési szabályok változása esetén, vagy a szervezet által meghatározott gyakorisággal megismerték és dokumentált módon elfogadták az aktuális hozzáférési szabályokat az EIR-ekhez való hozzáférés megtartása érdekében.

MAGYARÁZAT

A hozzáférési szabályok magukban foglalják a titoktartási megállapodásokat, az elfogadható használati megállapodásokat, a viselkedési szabályokat. Az aláírt hozzáférési megállapodások tartalmazzák annak elismerését, hogy az egyének elolvasták, megértették és egyetértenek azzal, hogy betartják a korlátozásokat, amelyek az érintett szervezet EIR-jeihez való hozzáféréssel járnak. Az érintett szervezet elektronikus aláírásokat használhat a hozzáférési megállapodások elismerésére, kivéve, ha azt az érintett szervezet valamely szabályzata ezt kifejezetten tiltja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia és dokumentálnia kell az EIR-ekhez való hozzáférés szabályait.

2. A szervezetnek a szervezet által meghatározott gyakorisággal felül kell vizsgálnia és frissítenie kell a hozzáférési szabályokat, hogy biztosítsa azok naprakészségét és relevanciáját.

3. A szervezetnek ellenőriznie kell, hogy az EIR-ekhez hozzáférést igénylő személyek megismerték és dokumentált módon elfogadták a vonatkozó hozzáférési szabályokat a hozzáférés megadása előtt. Amennyiben a hozzáférési szabályok változnak, (vagy a szervezet által meghatározott gyakorisággal, vagy meghatározott esetekben) a szervezetnek biztosítania kell, hogy az EIR-ekhez hozzáférést igénylő személyek megismerték és dokumentált módon

elfogadták az aktuális hozzáférési szabályokat az EIR-ekhez való hozzáférés megtartása érdekében.

5. A szervezetnek dokumentálnia kell a fenti folyamatot.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.100. Távoli hozzáférés

12.2. A fizikai belépési engedélyek

13.3.1. Viselkedési szabályok

14.2. Munkakörök biztonsági szempontú besorolása

14.3. Személyek háttérellenőrzése

14.9. Hozzáférési megállapodások

14.11. Külső személyekhez kapcsolódó biztonsági követelmények

14.12. Fegyelmi intézkedések

16.98. Külső fejlesztők háttérellenőrzése

18.67. Információ kezelése és megőrzése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.5.4; A.5.14; A.6.2; A.6.6

NIST SP 800-53 REV.5 REFERENCIA

PS-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

14.10. Hozzáférési megállapodások – Munkaviszony megszűnése után is fennálló kötelezettségek

14.10. A szervezet:

14.10.1. Tájékoztatja az egyéneket a munkaviszonyuk megszűnése után is érvényes, jogilag kötelező információvédelmi követelményekről.

14.10.2. Megköveteli az egyénektől, hogy aláírásukkal elismerjék ezeket a követelményeket, mielőtt először hozzáférnének a védett információkhoz.

Magyarázat

Ezek a követelmények jogi értelemben is kötelező információvédelmi előírásokat tartalmaznak, amelyek a személyekre nézve is érvényesek, még a munkaviszonyuk megszűnése után is. Az érintett szervezet felelőssége, hogy tájékoztassa az egyéneket ezekről a követelményekről.

A követelmény alkalmazásának lépései

1. A szervezetnek konzultálnia kell a jogi szakértőjével vagy jogi osztályával a munkaviszony megszűnése után érvényes, jogilag is kikényszeríthető kötelezettségekkel kapcsolatos kérdésekben.
2. A szervezetnek tájékoztatnia kell az egyéneket a munkaviszonyuk megszűnése után is érvényes, jogilag kötelező információvédelmi követelményekről.
3. A szervezetnek meg kell követelnie az egyénektől, hogy aláírásukkal elismerjék ezeket a követelményeket, mielőtt először hozzáférnének az EIR-ben tárolt védett információkhoz.
4. A szervezetnek biztosítania kell, hogy az EIR-ben tárolt információkhoz való hozzáférés naplózva legyen, és rendszeresen ellenőrizze a naplókat, hogy biztosítsa a követelmények betartását.
5. A szervezetnek szankciókat kell bevezetnie azok számára, akik nem tartják be ezeket a követelményeket, beleértve a munkaviszony megszűnését és további jogi következményeket.
6. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell az információvédelmi szabályzatait és eljárásrendjeit.

Kapcsolódó intézkedések

14.5. Személyek munkaviszonyának megszűnése

41/2015. (VII. 15.) BM RENDELETI REFERENCIA

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

PS-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

14.11. KÜLSŐ SZEMÉLYEKHEZ KAPCSOLÓDÓ BIZTONSÁGI KÖVETELMÉNYEK

14.11. A szervezet:

14.11.1. Személyi biztonsági követelményeket állít fel a külső szolgáltatókkal szemben, amelyek magukba foglalják a szükséges biztonsági szerepköröket és felelősségeket.

14.11.2. Megköveteli a külső szolgáltatóktól, hogy tartsák be a szervezet által meghatározott személyi biztonsági szabályokat.

14.11.3. Dokumentálja a személyi biztonsági követelményeket.

14.11.4. Megköveteli a külső szolgáltatóktól, hogy a meghatározott időn belül értesítsék a meghatározott személyeket vagy szerepköröket minden olyan külső személy áthelyezéséről vagy kilépéséről, akik szervezeti hitelesítő eszközzel, belépőkártyával vagy rendszerjogosultsággal rendelkeztek.

14.11.5. Ellenőrzi, hogy a szolgáltató megfelel-e a személyi biztonsági követelményeknek.

MAGYARÁZAT

A külső szolgáltató kifejezés olyan szervezetekre utal, amelyek nem közvetlenül az EIR-t üzemeltető vagy azt beszerző szervezetek. A külső szolgáltatók közé tartoznak a szerződéses partnerek és más szervezetek, amelyek rendszerfejlesztést, informatikai szolgáltatásokat, tesztelési vagy értékelési szolgáltatásokat, kiszervezett alkalmazásokat és hálózatkezelést nyújtanak stb.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a személyi biztonsági követelményeket a külső szolgáltatók számára. Ezeknek a követelményeknek tartalmazniuk kell a szükséges biztonsági szerep- és felelősségeket.
2. A szervezetnek meg kell követelnie a külső szolgáltatóktól, hogy tartsák be a szervezet által meghatározott személyi biztonsági szabályokat.
3. A szervezetnek dokumentálnia kell a személyi biztonsági követelményeket, hogy biztosítsa azok átláthatóságát és nyomon követhetőségét.

4. A szervezetnek meg kell követelnie a külső szolgáltatóktól, hogy a meghatározott időn belül értesítsék a meghatározott személyeket vagy szerepköröket minden olyan külső személy áthelyezéséről vagy kilépéséről, akik EIR hitelesítő eszközzel, belépőkártyával vagy EIR jogosultsággal rendelkeztek.
5. A szervezetnek ellenőriznie kell, hogy a szolgáltató megfelel-e a személyi biztonsági követelményeknek. Ez magában foglalhatja a szolgáltató által készített dokumentáció, jegyzőkönyvek és naplók vizsgálatát, valamint a személyi biztonsági szabályok betartásának ellenőrzését.
6. Amennyiben a szolgáltató nem felel meg a személyi biztonsági követelményeknek, a szervezetnek intézkedéseket kell hoznia a helyzet javítása érdekében, amely magában foglalhatja a szolgáltatóval való szerződés felülvizsgálatát vagy megszüntetését.

Kapcsolódó intézkedések

3.2. Biztonságtudatossági képzés
3.9. Szerepkör alapú biztonsági képzés
10.18. Karbantartó személyek
12.6. A fizikai belépés ellenőrzése
14.2. Munkakörök biztonsági szempontú besorolása
14.3. Személyek háttérellenőrzése
14.5. Személyek munkaviszonyának megszűnése
14.8. Az áthelyezések, átirányítások és kirendelések kezelése
14.9. Hozzáférési megállapodások
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.2; A.5.4

NIST SP 800-53 rev.5 referencia

PS-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

14.12. FEGYELMI INTÉZKEDÉSEK

14.12. A szervezet:

14.12.1. Fegyelmi eljárást kezdeményez azokkal az egyénekkel szemben, akik nem tartják be az információbiztonsági szabályokat és eljárásokat.

14.12.2. Meghatározott időn belül értesíti a szervezet által meghatározott személyeket vagy szerepköröket, amikor fegyelmi eljárás kerül megindításra, azonosítva az eljárás alá vont személyt és az eljárás okát.

MAGYARÁZAT

A fegyelmi eljárások lehetséges szankciót az hozzáférési megállapodásokban írják le, és általános személyi biztonsági szabályok részét képezhetik a szervezeteknél vagy meghatározhatók a biztonsági szabályokban. Amikor fegyelmi eljárás kerül megindításra, az érintett szervezet meghatározott időn belül értesíti a szervezet által meghatározott személyeket vagy szerepköröket. Az értesítésben azonosítják az eljárás alá vont személyt és az eljárás okát. Fontos, hogy az érintett szervezetben mindenki tisztában legyen azzal, hogy az EIR szabályok és eljárások megsértése komoly következményekkel járhat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia a fegyelmi eljárás intézményét saját magán belül, amelyet alkalmaznak azokkal az egyénekkel szemben, akik nem tartják be az EIR biztonsági szabályokat és eljárásokat. Ez a fegyelmi eljárás összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
2. A szervezetnek be kell építenie a szankciók folyamatát a hozzáférési megállapodásokba, és ezeket a szankciókat be kell foglalni a szervezet általános személyi szabályzataiba és/vagy a szervezet információbiztonsági szabályzataiba.
3. A szervezetnek dokumentálnia kell a fegyelmi eljárásokat, beleértve az érintett személyeket, az eljárás okát és az értesítés időpontját. Ez a napló segít az érintett szervezetnek nyomon követni és értékelni a fegyelmi eljárások hatékonyságát.

Kapcsolódó intézkedések

13.3.1. Viselkedési szabályok

1.13. Belső fenyegetés elleni program

14.9. Hozzáférési megállapodások

41/2015. (VII. 15.) BM rendeleti referencia

3.1.6.7. Fegyelmi intézkedések

ISO/IEC 27001:2023 referencia

7.3; A.6.4

NIST SP 800-53 rev.5 referencia

PS-8

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

14.13. MUNKAKÖRI LEÍRÁSOK

14.13. A szervezet belefoglalja a biztonsági szerepköröket és felelősségeket a szervezeti munkaköri leírásokba.

MAGYARÁZAT

A biztonsági szerepkörök meghatározása az egyes szervezeti munkaköri leírásokban elősegíti a szerepkörökkel kapcsolatos biztonsági felelősségek, valamint a szerepkör alapú biztonsági képzési követelmények megértését. Az érintett szervezetnek fontos, hogy a munkaköri leírásokban tisztázza a biztonsági szerepköröket és felelősségeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági szerep- és felelősségi köröket, amelyek szükségesek a szervezeti vagyon, személyek és EIR biztonságának megőrzéséhez.
2. A szervezetnek bele kell foglalja ezeket a szerep- és felelősségi köröket a szervezeti munkaköri leírásokba. Ez magában foglalja a munkaköri leírások frissítését, hogy tükrözzék a biztonsági szerep- és felelősségi köröket, valamint az új munkaköri leírások létrehozását, ha szükséges.
3. A szervezetnek biztosítania kell, hogy minden alkalmazott, aki biztonsági szerepkörben dolgozik, megfelelő képzést kapjon. Ez magában foglalhatja a biztonsági szabályzatok és eljárásrendek, az EIR használatának legjobb gyakorlatai, a naplózás és a biztonsági események kezelésének képzését, de külső képzéseket is.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a munkaköri leírásokat, hogy biztosítsa azok naprakészségét, valamint, hogy tükrözzék a jelenlegi biztonsági szerep- és felelősségi köröket. Ez magában foglalhatja a munkaköri leírások éves felülvizsgálatát, vagy amikor jelentős változások történnek az EIR-ben vagy a biztonsági környezetben.
5. A szervezetnek dokumentálnia kell a biztonsági szerep- és felelősségi körökkel kapcsolatos tevékenységeket, hogy bizonyítékot szolgáltasson a megfelelőségről és segítse az esetleges biztonsági problémák azonosításában és kezelésében.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

41/2015. (VII. 15.) BM rendeleti referencia

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.2

NIST SP 800-53 rev.5 referencia

PS-9

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024