Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Fizikai és környezeti védelem

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

12.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

12.1. A szervezet:

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

12.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó fizikai védelmi szabályzatot, amely

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

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

12.1.1.2. a fizikai és környezeti védelemre vonatkozó eljárásrendet, amely a fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

12.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a fizikai védelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

12.1.3. Felülvizsgálja és frissíti az aktuális fizikai védelmi szabályzatot és a fizikai és környezeti védelemre vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A fizikai védelmi 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 fizikai védelmi szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a fizikai védelmi 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 fizikai védelmi 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 fizikai védelmi szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

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

3.2.1.2. Fizikai védelmi eljárásrend

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

PE-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.2. A FIZIKAI BELÉPÉSI ENGEDÉLYEK

12.2. A szervezet

12.2.1. Összeállítja, jóváhagyja és kezeli az EIR-eknek helyet adó létesítményekbe belépésre jogosultak listáját.

12.2.2. Belépési jogosultságot igazoló dokumentumokat, hitelesítő eszközöket (például: kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépni szándékozó részére.

12.2.3. A szervezeti előírások szerinti gyakorisággal rendszeresen felülvizsgálja a belépésre jogosult személyek listáját.

12.2.4. Eltávolítja a belépésre jogosult személyek listájáról azokat, akik már nem jogosultak a belépésre.

MAGYARÁZAT

A fizikai belépési engedélyek a munkavállalókra és a látogatókra egyaránt vonatkoznak. Azokat a személyeket, akiknek folyamatosan fennálló fizikai belépési engedélyük van, nem tekinthetők látogatóknak. A hitelesítő eszközök közé tartoznak a kitűzők, azonosító kártyák és intelligens kártyák. Az érintett szervezet a belépési jogosultságokat a vonatkozó jogszabályok, irányelvek, szabályok, szabványok és útmutatókkal összhangban határozza meg. Az érintett szervezetnek lehetnek olyan, bárki által megközelíthető területei, melyek esetében nincs szükség fizikai belépési engedélyre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek össze kell állítania, jóvá kell hagynia és karban kell tartania egy listát azokról, akik jogosultak belépni az EIR-eknek helyt adó létesítményekbe.
2. A szervezetnek belépési jogosultságot igazoló dokumentumokat, hitelesítő eszközöket kell kibocsátania a belépni szándékozó részére.
3. A szervezetnek a szervezeti előírások szerinti gyakorisággal rendszeresen felül kell vizsgálnia a belépésre jogosult személyek listáját.
4. A szervezetnek el kell távolítania a belépésre jogosult személyek listájáról azokat, akik már nem jogosultak a belépésre.
5. A szervezetnek a belépési jogosultságokat a vonatkozó jogszabályokkal, irányelvekkel, szabályokkal, szabványokkal és útmutatókkal összhangban kell meghatároznia.

6. A szervezetnek lehetnek olyan, bárki által megközelíthető (nyilvános zónába tartozó) területei, melyek esetében nincs szükség fizikai belépési engedélyre.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

4.25. Naplóinformációk védelme

8.14. Azonosító kezelés

10.18. Karbantartó személyek

11.2. Hozzáférés az adathordozókhoz

12.6. A fizikai belépés ellenőrzése

12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

12.15. A kimeneti eszközök hozzáférés-ellenőrzése

12.22. Látogatói hozzáférési naplók

1.13. Belső fenyegetés elleni program

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

3.2.1.3. Fizikai belépési engedélyek

ISO/IEC 27001:2023 referencia

A.7.2

NIST SP 800-53 rev.5 referencia

PE-2

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.3. Fizikai belépési engedélyek – Szerep- vagy feladatkör alapú hozzáférés

12.3. A szervezet szerepkör vagy beosztás alapján engedélyezi a fizikai belépést az EIR-nek helyet adó létesítménybe.

Magyarázat

A szerepkör vagy beosztás alapú fizikai belépéshez sorolható az állandó karbantartó személyzet, biztonsági őrök, illetve a sürgősségi orvosi személyzet részére kibocsátott állandó fizikai belépési engedély.

A követelmény alkalmazásának lépései

A szervezetnek meg kell határoznia, mely szerepkörben vagy beosztásban dolgozó egyének rendelkeznek fizikai belépési engedéllyel az EIR-nek helyt adó létesítménybe.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.60. Legkisebb jogosultság elve

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

PE-2(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.4. Fizikai belépési engedélyek – Kétféle azonosító megléte

12.4. A szervezet előírja, hogy a látogatóknak kétféle, a szervezet által meghatározott és elfogadott azonosító okmányt kell bemutatniuk az EIR-nek helyet adó létesítménybe történő belépéshez. A szervezet határozza meg az általa elfogadhatónak ítélt azonosító okmányok listáját.

Magyarázat

Az elfogadható azonosító okmányok közé tartozhatnak az útlevelek, a vezetői engedélyek, és a személyazonosító igazolványok. Az EIR-nek helyt adó létesítménybe történő belépés megkönnyítése érdekében az érintett szervezet személyazonosságot igazoló kártyákat, kulcskártyákat, PIN kódokat és biometrikus adatokat igénylő beléptetőrendszert is használhat automatizált mechanizmusként.

A követelmény alkalmazásának lépései

A szervezetnek elő kell írnia, hogy a látogatóknak kétféle azonosító okmányt kell bemutatniuk az EIR-nek helyt adó létesítménybe történő belépéshez.

Kapcsolódó intézkedések

8.2. Azonosítás és hitelesítés

8.14. Azonosító kezelés

8.21. A hitelesítésre szolgáló eszközök kezelése

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

PE-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az az elfogadható személyazonosító okmányokra vonatkozó lista meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.5. Fizikai belépési engedélyek – Kíséret nélküli hozzáférés korlátozása

12.5. A szervezet a szükséges biztonsági ellenőrzéssel és hozzáférési jogosultsággal rendelkező személyzetre korlátozza a kíséret nélküli fizikai belépést az EIR-nek helyet adó létesítmény területére.

Magyarázat

Azok a személyek, akik nem rendelkeznek a szükséges biztonsági engedélyekkel, belépési jogosultságokkal, csak olyan személyek kíséretében léphetnek be az EIR-nek helyt adó létesítmény területére, akik rendelkeznek a megfelelő fizikai hozzáférési engedélyekkel. Az érintett szervezet így biztosítja, hogy a szükséges biztonsági engedélyekkel, belépési jogosultságokkal nem rendelkező személyek ne férhessenek hozzá jogosulatlanul a szervezetet érintő információkhoz.

A követelmény alkalmazásának lépései

1. A szervezetnek alkalmaznia kell egy rendszert, amely korlátozza a kíséret nélküli fizikai belépést az EIR-nek helyt adó létesítmény területére.
2. A szervezetnek biztosítania kell, hogy azok a személyek, akik nem rendelkeznek a szükséges biztonsági engedélyekkel, belépési jogosultságokkal, csak olyan személyek kíséretében léphetnek be az EIR-nek helyt adó létesítmény területére, akik rendelkeznek a megfelelő fizikai hozzáférési engedélyekkel.

Kapcsolódó intézkedések

14.2. Munkakörök biztonsági szempontú besorolása

14.9. Hozzáférési megállapodások

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

PE-2(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a fizikai belépési engedélyek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.6. A FIZIKAI BELÉPÉS ELLENŐRZÉSE

12.6. A szervezet:

12.6.1. Kizárólag a szervezet által meghatározott be- és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést.

12.6.1.1. Ellenőrzi az egyéni jogosultságokat a létesítménybe való belépés előtt.

12.6.1.2. Ellenőrzi a létesítménybe való be- és kilépést a meghatározott fizikai beléptető rendszerek vagy eszközök illetve őrök segítségével.

12.6.2. Naplózza a fizikai be- illetve kilépéseket.

12.6.3. Ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket.

12.6.4. Kíséri a létesítménybe ad hoc belépésre jogosultakat, és figyelemmel követi a tevékenységüket.

12.6.5. Megóvja a kulcsokat, hozzáférési kódokat és az egyéb fizikai hozzáférést biztosító eszközöket.

12.6.6. Nyilvántartást vezet a fizikai belépést ellenőrző eszközökről, és meghatározott gyakorisággal frissíti azt.

12.6.7. Meghatározott rendszerességgel megváltoztatja a hozzáférési kódokat és kulcsokat, illetve, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az azokkal rendelkező személy elveszíti a belépési jogosultságát.

MAGYARÁZAT

A fizikai hozzáférésre vonatkozó elvárások a munkavállalókra és a látogatókra egyaránt alkalmazandóak. Az állandó fizikai hozzáférési jogosultsággal rendelkező személyek nem minősülnek látogatónak. A nyilvános területek fizikai hozzáférés felügyelete magában foglalhatja a fizikai hozzáférések rögzítését, az őröket vagy a fizikai hozzáférést korlátozó eszközöket és sorompókat, amelyek meggátolják a bejutást a nyilvánosan hozzáférhető területekről a nem nyilvános területekre. Az érintett szervezet meghatározza milyen őrző-védő személyzetre van szükség pl.: hivatásos biztonsági személyzet, rendszer felhasználói, adminisztratív személyzet. Fizikai hozzáférési eszközökhöz soroljuk a kulcsokat, a zárakat, a számkombinációkat, biometrikus és kártyaolvasókat. A fizikai hozzáférés felügyeletét elvégző rendszereknek meg kell felelniük a vonatkozó törvényeknek, végrehajtási rendeleteknek,

irányelveknek, előírásoknak, szabványoknak és ajánlásoknak. A szervezetek rugalmasan dönthetnek arról, hogy milyen módon valósítják meg a fizikai hozzáférésekre vonatkozó bejegyzések kezelésére alkalmazott különböző naplóbejegyzéseket. A bejegyzések készülhetnek valamilyen eljárás során, automatikusan vagy ezek valamilyen kombinációjával. A fizikai hozzáférési pontok magukban foglalhatják a létesítmény ki- és belépési pontjait, a rendszerek belső hozzáférési pontjait, amelyek további hozzáférésellenőrzést igényelhetnek. A rendszer elemei elhelyezhetőek a szervezet által meghatározott publikus zónában, amennyiben a szervezet ellenőrzi a rendszerelemekhez történő hozzáférést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek kizárólag az általa meghatározott be- és kilépési pontokon szabad biztosítania a belépésre jogosultak számára a fizikai belépést.
2. A szervezetnek ellenőriznie kell az egyéni jogosultságokat a létesítménybe való belépés előtt. Ez magában foglalhatja a személyazonosság ellenőrzését, a belépési jogosultságok ellenőrzését, és a belépési kódok vagy kulcsok ellenőrzését.
3. A szervezetnek ellenőriznie kell a létesítménybe való be- és kilépést a meghatározott fizikai beléptető rendszerek vagy eszközök, illetve őrök segítségével.
4. A szervezetnek naplóznia kell a fizikai be- és kilépéseket. Ez magában foglalhatja a belépés és kilépés idejének, a belépő és kilépő személyek, illetve a belépési és kilépési események rögzítését.
5. A szervezetnek ellenőrzés alatt kell tartania a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket.
6. A szervezetnek kísérnie kell a létesítménybe ad hoc belépésre jogosultakat, és figyelemmel kell követnie a tevékenységüket.
7. A szervezetnek meg kell óvnia a kulcsokat, hozzáférési kódokat és az egyéb fizikai hozzáférést biztosító eszközöket. Ez magában foglalhatja a kulcsok, hozzáférési kódok és eszközök tárolását, ellenőrzését és karbantartását.
8. A szervezetnek nyilvántartást kell vezetnie a fizikai belépést ellenőrző eszközökről, és meghatározott gyakorisággal frissítenie kell azokat.

9. A szervezetnek meghatározott rendszerességgel meg kell változtatnia a hozzáférési kódokat és kulcsokat, illetve, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az azokkal rendelkező személy elveszíti a belépési jogosultságát.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.25. Naplóinformációk védelme

4.44. Információk kiszivárgásának figyelemmel kísérése

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

8.10. Eszközök azonosítása és hitelesítése

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

10.18. Karbantartó személyek

11.2. Hozzáférés az adathordozókhoz

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

3.2.1.4. A fizikai belépés ellenőrzése

ISO/IEC 27001:2023 referencia

A.7.1; A.7.2; A.7.3; A.7.4

NIST SP 800-53 rev.5 referencia

PE-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.7. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – RENDSZER HOZZÁFÉRÉS

12.7. A szervezet a létesítménybe történő fizikai belépés ellenőrzésén túlmenően külön engedélyhez köti a fizikai belépést a szervezet által meghatározott fizikai helyiségekbe, amelyek egy vagy több rendszerelemet tartalmaznak.

MAGYARÁZAT

Az érintett szervezet a létesítménybe történő fizikai belépés ellenőrzésén túlmenően külön engedélyhez köti a fizikai belépést a szervezet által meghatározott fizikai helyiségekbe, amelyek egy vagy több rendszerelemet tartalmaznak. Ez az EIR szempontjából további fizikai biztonsági réteget jelent.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a fizikai helyiségeket, ahol egy vagy több rendszerelem található.
2. A szervezetnek külön engedélyhez kell kötnie a fizikai belépést a szervezet által meghatározott fizikai helyiségekbe, amelyek egy vagy több rendszerelemet tartalmaznak.
3. A szervezetnek biztosítania kell, hogy a fizikai belépési engedélyezési rendszer működik és hatékonyan ellenőrzi a belépést a meghatározott helyiségekbe.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.2.1.4. A fizikai belépés ellenőrzése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

PE-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer egy vagy több elemét tartalmazó fizikai helyszín meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

12.8. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – LÉTESÍTMÉNY ÉS RENDSZEREK

12.8. A szervezet meghatározott gyakorisággal biztonsági ellenőrzéseket végez a létesítmény vagy rendszer fizikai határain annak érdekében, hogy megakadályozza az információk kiszivárogtatását vagy a rendszerelemek eltávolítását.

MAGYARÁZAT

A fizikai határokon végzett ellenőrzésekkel az érintett szervezet csökkentheti az információk kiszivárgásának, ill. a rendszerelemek jogosulatlan eltávolításának kockázatát. Az ellenőrzések gyakoriságának meghatározását a kockázattal arányos védelem elvét figyelembe véve célszerű végrehajtani.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meghatározott gyakorisággal biztonsági ellenőrzéseket kell végeznie a létesítmény vagy rendszer fizikai határain annak érdekében, hogy megakadályozza az információk kiszivárogtatását vagy a rendszerelemek eltávolítását.
2. A szervezetnek ki kell dolgoznia és be kell vezetnie egy biztonsági ellenőrzéssel kapcsolatos eljárásrendet, amely magában foglalja az EIR fizikai határainak ellenőrzését.
3. A szervezetnek dokumentálnia kell az összes biztonsági ellenőrzést, így nyomon követheti azokat.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a biztonsági ellenőrzési eljárásrendet, így biztosítva annak hatékonyságát és relevanciáját.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.28. Információáramlási szabályok érvényesítése

17.17. A határok védelme

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.12

NIST SP 800-53 REV.5 REFERENCIA

PE-3(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.9. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – FOLYAMATOS ÉLŐERŐS FELÜGYELET

12.9. A szervezet az EIR-nek helyet adó létesítménynek meghatározott fizikai hozzáférési pontjain 24 órás őrszolgálatot biztosít a hét minden napján.

MAGYARÁZAT

Az őrszolgálat biztosítása az EIR-t tartalmazó létesítmény meghatározott fizikai hozzáférési pontjain lehetővé teszi a gyorsabb reagálási képességet az érintett szervezet számára. Az őrök továbbá élőerős felügyeletet biztosítanak azokon a létesítményhez köthető területeken, amelyeket nem fed le a videós megfigyelés.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-nek helyet adó létesítmény fizikai hozzáférési pontjait. Ezek lehetnek bejáratok, kijáratok, vagy bármely olyan pont, ahol a személyek hozzáférhetnek az EIR-hez.
2. Miután a szervezet meghatározta a hozzáférési pontokat, szükség van egy 24 órás őrszolgálat kialakítására.
3. A szervezetnek gondoskodnia kell arról, hogy az őrök megfelelően képzettek legyenek a fizikai biztonsági eljárások ismeretanyagában. Ez jelentheti a gyanús tevékenységekre történő reagálást, a hozzáférési jogosultságok ellenőrzését és a fizikai belépések dokumentálását.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az őrszolgálati eljárásokat, hogy biztosítsa azok hatékonyságát és naprakészségét.
5. A szervezetnek biztosítania kell, hogy a fizikai biztonsági intézkedések összhangban vannak az EIR kiberbiztonsági követelményeivel. Ez azt jelenti, hogy a fizikai biztonsági intézkedéseknek támogatniuk kell az EIR biztonságát, és nem szabad, hogy akadályozzák az EIR hatékony működését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.19. Biztonsági tárolási helyszín

7.23. Alternatív feldolgozási helyszín

12.17. A fizikai hozzáférések felügyelete

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.7.4

NIST SP 800-53 REV.5 REFERENCIA

PE-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a fizikai belépési pontok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.10. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – ZÁRHATÓ HÁZAK VAGY BURKOLATOK

12.10. A szervezet a meghatározott rendszerelemek védelmében zárható fizikai házat vagy egyéb burkolatot alkalmaz a jogosulatlan fizikai hozzáférés megakadályozására.

MAGYARÁZAT

A legnagyobb kockázatot a hordozható eszközök (laptopok, okostelefonok, tabletek stb.) vonatkozásában a lopás jelenti. Az érintett szervezet alkalmazhat zárható fizikai házat vagy burkolatot a berendezések lopásával járó kockázat csökkentésére. Az ilyen házak számos méretben kaphatók, egyszerű notebookok védelmére szolgáló egységektől kezdve, egészen olyan szekrényekig, amelyek több szerver, számítógép és periféria védelmét is biztosítják. A zárható fizikai házakat vagy burkolatokat kábelzárakkal vagy lezáró lemezekkel együtt lehet használni, hogy megakadályozzák a számítógépes berendezést tartalmazó zárható ház vagy burkolat lopását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat az eszközöket, melyek ki vannak téve a jogosulatlan fizikai hozzáférés kockázatának.
2. Miután a szervezet azonosította az említett eszközöket, ki kell választania a megfelelő zárható fizikai házat vagy egyéb burkolatot, mely segít csökkenteni a jogosulatlan fizikai hozzáférés kockázatát.
3. A szervezetnek be kell szereznie a kiválasztott zárható fizikai házat vagy burkolatot.
4. A szervezetnek alkalmaznia kell a zárható fizikai házat vagy burkolatot, hogy védje az EIR-hez köthető rendszerelemeket a jogosulatlan fizikai hozzáféréstől. Ez magában foglalhatja a burkolatok rögzítését, a zárak beállítását és a kulcsok kezelését.
5. A szervezetnek dokumentálnia kell a zárható fizikai házak vagy burkolatok telepítését és használatát. A dokumentáció tartalmazhatja a telepítés dátumát, a kiválasztott védelmi eszköz használatát és a kulcsok kiadását.
6. A szervezetnek rendszeresen ellenőriznie kell a zárható fizikai ház vagy burkolat állapotát és működését.

7. A szervezetnek karban kell tartania a zárható fizikai házakat vagy burkolatokat. Ez érintheti az említett eszközök cseréjét, a zárak vagy a kulcsok cseréjét vagy javítását.

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

PE-3(4)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

12.11. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – MANIPULÁCIÓ ELLENI VÉDELEM

12.11. A szervezet meghatározott manipuláció elleni technológiákat alkalmaz a fizikai beavatkozások vagy módosítások észlelésének és megakadályozásának érdekében a szervezet által meghatározott rendszerelemeken.

MAGYARÁZAT

Az érintett szervezet meghatározza azokat a rendszerelemeket, amelyeknél a manipuláció észlelésére és megakadályozására valamilyen megoldást kíván alkalmazni. A manipuláció elleni védelem segít az érintett szervezetnek abban, hogy észlelje és megakadályozza a nem kívánt vagy jogosulatlan fizikai beavatkozásokat a meghatározott rendszerelemeken. Emellett abban is segíti a szervezetet, hogy észlelje a hardverelemek hamisítását vagy más ellátási láncokkal kapcsolatos kockázatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely rendszerelemeknél alkalmazza a manipuláció elleni védelmet.
2. A szervezetnek ki kell választania és be kell szereznie a megfelelő manipuláció elleni technológiákat.
3. A szervezetnek alkalmaznia kell ezeket a technológiákat a meghatározott rendszerelemeken.
4. A szervezetnek dokumentálnia kell a manipuláció elleni védelemmel kapcsolatos tevékenységeket, beleértve az észlelt manipulációkat és a hozzájuk kapcsolódó intézkedéseket.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a manipuláció elleni védelmi intézkedéseit, hogy biztosítsa azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.86. Szoftverfejlesztők oktatása

19.20. Hamisítás elleni védelem

19.23. Rendszerelem hitelessége

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

PE-3(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a manipuláció elleni technológiák illetve az hardverelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.12. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – FIZIKAI AKADÁLYOK

12.12. A szervezet fizikai akadályok használatával korlátozza a különböző területekhez való hozzáférést.

MAGYARÁZAT

A fizikai akadályokra néhány példa: terelő- és lezáró oszlopok, betonkockák, terelőfalak, aktív hidraulikus járműoszlopok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a területeket, ahol a fizikai belépést fizikai akadályok segítségével korlátozni kívánja a belépést vagy járművel behajtást.
2. A szervezetnek el kell helyeznie a fizikai akadályokat.
3. A szervezetnek meg kell bizonyosodnia arról, hogy a fizikai akadályokat megfelelően telepítették és azok rendeltetésszerűen működnek. Ez jelentheti például a fizikai akadályok rendszeres ellenőrzését és azok karbantartását.
4. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a fizikai akadályok hatékonyságát. Amennyiben szükséges, az érintett szervezetnek meg kell tennie a szükséges intézkedéseket a fizikai adályok hatékonyságának biztosítására.

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

PE-3(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.13. A FIZIKAI BELÉPÉS ELLENŐRZÉSE – BELÉPTETŐ HELYISÉGEK

12.13. A szervezet hozzáférés-ellenőrző előtereket használ az általa meghatározott helyszíneken a létesítményeken belül.

MAGYARÁZAT

Az hozzáférés-ellenőrző előtér egy fizikai hozzáférés-ellenőrző rendszer része, amely tipikusan egy teret biztosít két zsilipelt beléptetőrendszer között. Az előtereket úgy tervezték, hogy megakadályozzák a fizikai belépési jogosultsággal nem rendelkező személyeket abban, hogy a fizikai belépési jogosultsággal rendelkező személyeket követve belépjenek a létesítménybe. Ez a tevékenység jogosulatlan belépést eredményez a létesítménybe. A zsilipelt beléptetőket arra használja az érintett szervezet, hogy korlátozza azoknak az egyéneknek a számát, akik belépnek az ellenőrzött belépési pontokra, és várakozásra fenntartott területeket biztosít, amíg a fizikai belépési engedélyt ellenőrzi. A zsilipelt beléptetők teljesen automatizáltak lehetnek (pl.: ellenőrzik az ajtók nyitását és zárását) vagy részben automatizáltak (pl.: biztonsági őröket használnak az előtérbe belépő személyek számának ellenőrzésére).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a helyszíneket a létesítményeiben, ahol hozzáférés-ellenőrző előtereket hoz létre.
2. A szervezetnek meg kell terveznie és létre kell hoznia a hozzáférés-ellenőrző előtereket. Ezek teret biztosítanak két zsilipelt beléptetőrendszer között, amely megakadályozza a fizikai belépési jogosultsággal nem rendelkező személyeket abban, hogy a fizikai belépési jogosultsággal rendelkező személyeket követve belépjenek a létesítménybe.
3. A szervezetnek zsilipelt beléptetőrendszereket kell alkalmaznia, melyek korlátozzák azoknak az egyéneknek a számát, akik belépnek az ellenőrzött belépési pontokra, és várakozásra fenntartott területeket biztosít, amíg a fizikai belépési engedélyt ellenőrzik. Alkalmazhat teljesen automatizált vagy részben automatizált (pl.: biztonsági őrök alkalmazása az előtérbe belépő személyek számának ellenőrzésére) zsilipelt beléptetőrendszert.

5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén módosítania kell a hozzáférés-ellenőrző előtereket és azok működését, így biztosítva azok hatékony működését.

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

PE-3(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az a létesítményen belüli helyszínek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.14. HOZZÁFÉRÉS AZ ADATÁTVITELI ESZKÖZÖKHÖZ ÉS CSATORNÁKHOZ

12.14. A szervezet meghatározott biztonsági követelményeket alkalmaz a fizikai hozzáférés szabályozására a saját létesítményeiben található meghatározott rendszerelosztókhoz (például: csatlakozók, elosztók) és átviteli vezetékekhez.

MAGYARÁZAT

Az adatátviteli eszközökhöz és csatornákhoz alkalmazott biztonsági intézkedések megakadályozzák a balesetből eredő károkat, zavarokat és fizikai manipulációkat. Az ilyen intézkedések szükségesek lehetnek a titkosítatlan kommunikáció lehallgatásának vagy módosításának megelőzéséhez. A rendszerelosztókhoz és átviteli vezetékekhez kapcsolódó fizikai hozzáférés szabályozására használt biztonsági intézkedések közé tartozik többek között a csatlakozóaljzatok leválasztása vagy lezárása, a zárt kábelrendezők, a kábelezés védelme védőcsővel vagy kábeltálcával, valamint a lehallgatás elleni érzékelők.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fizikai hozzáférési szabályokat a rendszerelosztókhoz és átviteli vezetékekhez.
2. A szervezetnek alkalmaznia kell a meghatározott biztonsági követelményeket a fizikai hozzáférés szabályozására a saját létesítményeiben található meghatározott rendszerelosztókhoz és átviteli vezetékekhez.
3. A szervezetnek továbbá biztosítania kell, hogy a fizikai hozzáférési szabályokat minden érintett alkalmazza és betartja. Ez magában foglalhatja a személyzet képzését és tájékoztatását a szabályokról, valamint a szabályok betartásának ellenőrzését.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a fizikai hozzáférési szabályokat, hogy biztosítsa azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.9. Szerepkör alapú biztonsági képzés

8.14. Azonosító kezelés

11.2. Hozzáférés az adathordozókhoz

11.4. Adathordozók tárolása

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

12.15. A kimeneti eszközök hozzáférés-ellenőrzése

12.24. Áramellátó berendezések és kábelezés

17.17. A határok védelme

17.40. Az adatátvitel bizalmassága és sértetlensége

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

3.2.1.5. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz: Az érintett szervezet az általa meghatározott biztonsági védelemmel ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

ISO/IEC 27001:2023 REFERENCIA

A.7.2; A.7.12

NIST SP 800-53 REV.5 REFERENCIA

PE-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelosztók és átviteli vezetékek illetve a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

12.15. A KIMENETI ESZKÖZÖK HOZZÁFÉRÉS-ELLENŐRZÉSE

12.15. A szervezet ellenőrzi az EIR kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek hozzá az előállított kimenetekhez.

MAGYARÁZAT

A kimeneti eszközökhöz való fizikai hozzáférés ellenőrzés magában foglalja a kimeneti eszközök zárt helyiségekben vagy egyéb kártyaolvasóval vagy tasztatúrával biztosított területeken való elhelyezését, ahol a hozzáférést csak az arra jogosult személyek számára biztosítja, továbbá a kimeneti eszközök elhelyezésére szolgáló helyiséget a szervezet személyzetének képesnek kell lennie ellenőrizni. Az érintett szervezetnek biztosítania kell monitor vagy képernyőszűrők és headsetek használatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR kimeneti eszközei zárt helyiségekben vagy egyéb kártyaolvasóval, illetve tasztatúrával biztosított területeken kerülnek elhelyezésre.
2. A szervezet a hozzáférést csak az arra jogosult személyek számára biztosítja.
3. A szervezetnek olyan helyeken kell elhelyeznie az EIR kimeneti eszközeit, ahol a személyzet képes azokat ellenőrizni.
4. A szervezetnek rendszeres időnként felül kell vizsgálnia az EIR kimeneti eszközeit tartalmazó helyiség belépési naplóit.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.2. A fizikai belépési engedélyek
12.6. A fizikai belépés ellenőrzése
12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz
12.44. Az információs rendszer elemeinek elhelyezése

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

3.2.1.6. A kimeneti eszközök hozzáférés ellenőrzése: Az érintett szervezet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.

ISO/IEC 27001:2023 REFERENCIA

A.7.2; A.7.3; A.7.7

NIST SP 800-53 REV.5 REFERENCIA

PE-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kimeneti eszközök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

12.16. A KIMENETI ESZKÖZÖK HOZZÁFÉRÉS-ELLENŐRZÉSE – SZEMÉLYAZONOSSÁGHOZ KAPCSOLHATÓSÁG

12.16. A szervezet a kimeneti eszközökből származó információk fogadását vagy átvételét a fogadó vagy átvevő személy azonosításhoz köti.

MAGYARÁZAT

Az érintett szervezet biztosítja, hogy a kimeneti eszközökből származó információk fogadására vagy átvételére csak azonosított személyek legyenek képesek. Ez azt jelenti, hogy a kimeneti eszköz képes azonosítani a felhasználókat, mielőtt hozzáférést biztosít számukra a kimeneti adatokhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a kimeneti eszközökből származó információk fogadására vagy átvételére csak azonosított személyek legyenek képesek.
2. A kimeneti eszköznek képesnek kell lennie azonosítani a felhasználókat, mielőtt hozzáférést biztosít számukra a kimeneti adatokhoz.

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

PE-5(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.17. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE

12.17. A szervezet:

12.17.1. Ellenőrzi a fizikai hozzáféréseket az EIR-eket tartalmazó létesítményekben, hogy észlelje a fizikai biztonsági eseményeket és reagáljon rájuk.

12.17.2. Rendszeresen átvizsgálja a fizikai hozzáférések naplóit, és azonnal áttekinti azokat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak.

12.17.3. Összehangolja az ellenőrzések, vizsgálatok eredményeit a szervezet eseménykezelési képességével.

MAGYARÁZAT

Az EIR-eket tartalmazó létesítményekben a fizikai hozzáférések felügyelete azt jelenti, hogy az érintett szervezet folyamatosan figyelemmel kíséri és észleli a fizikai biztonsági eseményeket, illetve szükség esetén reagál azokra. A fizikai hozzáférések felügyelete magában foglalja a bárki által hozzáférhető, az érintett szervezethez tartozó területek felügyeletét is. Az érintett szervezet a fizikai felügyeletet megvalósíthatja biztonsági őrök, biztonsági kamerák és egyéb érzékelő berendezések segítségével. Az érintett szervezet rendszeresen átvizsgálja a fizikai belépéssel kapcsolatos naplókat, és elemzi azokat, ha a rendelkezésre álló információk jogosulatlan fizikai belépési utalnak. Jogosulatlan fizikai belépésre utalhat a normál munkaórákon kívül eső belépés, a szokatlan ideig történő bent tartózkodás a létesítményben, ismételten végrehajtott belépések nem szokványos területekre és minden egyéb, a megszokott mintázattól eltérő belépés. Az ellenőrzések és vizsgálatok eredményeit az érintett szervezet összehangolja az eseménykezelési képességével, így hatékonyabban kezelheti a biztonsági eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ellenőriznie kell a fizikai hozzáféréseket az EIR-eket tartalmazó létesítményekben így képes lehet észlelni a fizikai biztonsági eseményeket és reagálni tud azokra.

2. A szervezetnek rendszeresen át kell vizsgálnia a fizikai hozzáférési naplókat. Ez segíthet a gyanús tevékenységek, a normális működéstől eltérő események vagy potenciális fenyegetések azonosításában.

3. A szervezetnek azonnal elemeznie kell a naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak.

4. A szervezetnek össze kell hangolnia az ellenőrzések és vizsgálatok eredményeit a szervezet eseménykezelési képességével.

Kapcsolódó intézkedések

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.25. Naplóinformációk védelme

4.40. Naplóbejegyzések létrehozása

5.14. Folyamatos felügyelet

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

9.9.1. Biztonsági események kezelése

9.34. Biztonsági eseménykezelési terv

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

3.2.1.7. A fizikai hozzáférések felügyelete

ISO/IEC 27001:2023 referencia

A.7.4; A.8.16

NIST SP 800-53 rev.5 referencia

PE-6

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.18. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE – BEHATOLÁSJELZŐ ÉS MEGFIGYELŐ BERENDEZÉSEK

12.18. A szervezet fizikai behatolásjelző és felügyeleti berendezések alkalmazásával ellenőrzi a fizikai hozzáférési pontokat az EIR-nek helyet adó létesítményekben.

MAGYARÁZAT

Az érintett szervezet fizikai behatolásjelzőket alkalmaz, melyek képesek figyelmeztetni a biztonsági személyzetet, amikor jogosulatlan hozzáférési kísérlet történik egy szervezeti létesítményhez. A riasztórendszerek kiegészítik a fizikai akadályok, a fizikai hozzáférés-ellenőrző rendszerek és a biztonsági őrök által biztosított őrző-védő szolgáltatás által biztosított védelmi funkciót. Jelezhetnek, amikor az említett biztonsági intézkedések nem elegendőek egy jogosulatlan fizikai belépés megakadályozására. A fizikai behatolásjelzők különböző típusú érzékelő eszközöket tartalmazhatnak. A felügyeleti berendezések alatt a kamerás megfigyelést értjük, amelyeket meghatározott pontokon telepítenek az EIR-nek helyt adó létesítményben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a fizikai hozzáférési pontokat a szervezeti létesítmény(ek)ben.
2. A szervezetnek fizikai behatolásjelzőket és megfigyelő berendezéseket (pl.: biztonsági kamera) kell telepítenie ezeken a hozzáférési pontokon, illetve egyéb a szervezet által meghatározott terület(ek)en.
3. A szervezetnek biztosítania kell, hogy a behatolásjelzők és a felügyeleti berendezések megfelelően működnek. Ez magában foglalja a rendszeres tesztelést és karbantartást.
4. A szervezetnek dokumentálnia kell minden riasztást és biztonsági eseményt. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a biztonsági eseményeket, és megállapítsa, hogy szükség van-e további intézkedésekre.
5. A szervezetnek folyamatosan felül kell vizsgálnia és szükség esetén frissítenie kell a fizikai biztonsági intézkedéseket, annak érdekében, hogy biztosítsa azok hatékonyságát és naprakészségét.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.2.1.7. A fizikai hozzáférések felügyelete

ISO/IEC 27001:2023 referencia

A.7.4

NIST SP 800-53 rev.5 referencia

PE-6(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

12.19. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE – AUTOMATIZÁLT BETÖRÉS FELISMERÉS VÁLASZADÁS

12.19. A szervezet képes felismerni a szervezet által meghatározott típusú behatolásokat, és a szervezet által meghatározott válaszintézkedések meghozatalát kezdeményezi a szervezet által meghatározott automatizált mechanizmusok használatával.

MAGYARÁZAT

A behatolásra adott válaszlépés magában foglalhatja a meghatározott szervezethez köthető személyek és/vagy a rendvédelmi szervek értesítését. A válaszlépések kezdeményezésére bevezetett automatizált mechanizmusok közé tartoznak a rendszerriasztással kapcsolatos értesítések, az e-mail-es és szöveges üzenetek, valamint az ajtózáró mechanizmusok aktiválása. A fizikai hozzáférés felügyelete összehangolható a behatolásérzékelő rendszerekkel és a rendszerfelügyeleti képességekkel, így a szervezet számára integrált lefedettséget biztosíthatnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fizikai hozzáféréshez köthető behatolások típusait, és azokra válaszintézkedéseket kell kidolgoznia.
2. A szervezetnek meg kell határoznia, hogy milyen automatizált mechanizmusokat szeretne használni.
3. A szervezetnek a válaszintézkedések kidolgozása során figyelembe kell vennie a meghatározott automatizált mechanizmusok használatát és azokat alkalmaznia kell a gyakorlatban.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az automatizált betörés felismerésre használt mechanizmusait, így biztosítva azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.13. Az EIR monitorozása

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

PE-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a meghatározott típusú behatolások illetve a válaszintézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.20. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE – KAMERÁS MEGFIGYELÉS

12.20. A szervezet:

12.20.1. Meghatározott működési területeken videómegfigyelést alkalmaz.

12.20.2. Meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet, amelyet a szervezet által meghatározott személyek és szerepkörök jóváhagynak.

12.20.3. Meghatározott időtartamig megőrzi a videófelvételeket.

MAGYARÁZAT

A kamerás megfigyelés a meghatározott területeken végzett tevékenység rögzítésére összpontosít, hogy azt később - amennyiben a körülmények ezt indokolják - felül lehessen vizsgálni. A videofelvételeket jellemzően a rendellenes események vagy biztonsági események észlelése céljából vizsgálják felül. A videófelvételek megfigyelése nem kötelező, bár a szervezetek dönthetnek úgy, hogy alkalmazzák. A videófelvételek rögzítése és megőrzése során jogi megfontolások merülhetnek fel, különösen, ha a megfigyelés nyilvános helyen történik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a videómegfigyelési rendszere megfelelően működik és a meghatározott területeket figyeli.
2. A szervezetnek rendszeresen felül kell vizsgálnia a biztonsági eseménykezelési tervét. Ez a felülvizsgálat magában foglalja a tervben szereplő személyek és szerepkörök jóváhagyását is.
3. A szervezetnek meg kell határoznia, hogy milyen hosszú ideig őrzi meg a videófelvételeket. Ennek során a szervezetnek figyelembe kell venni a jogszabályi előírásokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

PE-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.21. A FIZIKAI HOZZÁFÉRÉSEK FELÜGYELETE – RENDSZEREKHEZ VALÓ FIZIKAI HOZZÁFÉRÉS-ELLENŐRZÉSE

12.21. A szervezet a létesítménybe történő fizikai belépések ellenőrzésén túl külön figyelmet fordít az EIR egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépésekre.

MAGYARÁZAT

Az érintett szervezet nem csak a létesítménybe történő fizikai belépések ellenőrzésére fordít figyelmet, hanem különös gondot fordít azokra a helyiségekre, amelyek egy vagy több rendszerelemet tartalmaznak, mint a szerverszobák, adathordozók, kommunikációs központok. Ez azt jelenti, hogy az érintett szervezet kiemelt figyelmet szentel az olyan helyiségek számára, ahol az EIR egyes rendszerelemei találhatók. Az ilyen helyiség fizikai hozzáférésének felügyelete összehangolható a behatolásészlelő (IDS) és más rendszerfelügyeleti eszköz képességeivel, így az érintett szervezet teljeskörűbb és integrált védelmet építhet ki.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a helyiségeket, ahol az EIR egy vagy több eleme található.
2. A szervezetnek be kell vezetnie egy fizikai hozzáférés-ellenőrző rendszert, amely monitorozza és naplózza a belépéseket és kilépéseket ezekbe a helyiségekbe. Ez magában foglalhatja a belépőkártyák, biometrikus azonosítók vagy más hozzáférés-ellenőrző eszközök használatát.
3. A szervezetnek meg kell határoznia az EIR egy vagy több rendszerelemeét tartalmazó helyiségekbe belépni jogosultak listáját, melyet rendszeresen felül kell vizsgálnia és naprakészen kell tartania.
4. A szervezetnek lehetősége van összehangolnia a fizikai hozzáférés-felügyeletet a behatolásészlelő rendszerekkel és más rendszerfelügyeleti eszköz képességeivel, így az érintett szervezet teljeskörűbb védelmet építhet ki.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.2.1.7. A fizikai hozzáférések felügyelete

ISO/IEC 27001:2023 REFERENCIA

A.7.4

NIST SP 800-53 REV.5 REFERENCIA

PE-6(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer egy vagy több elemét tartalmazó fizikai helyszín meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

12.22. LÁTOGATÓI HOZZÁFÉRÉSI NAPLÓK

12.22. A szervezet:

12.22.1. Meghatározott ideig megőrzi az EIR-eknek helyet adó létesítményekbe történt látogatói belépésekről szóló információkat.

12.22.2. Meghatározott gyakorisággal felülvizsgálja a látogatói belépésekről szóló nyilvántartást.

12.22.3. A látogatói belépésekről szóló nyilvántartásban észlelt rendellenességeket azonnal jelenti a meghatározott személynek vagy szerepkörnek.

MAGYARÁZAT

A látogatók belépési nyilvántartása tartalmazza a látogató személy nevét és a képviselt szervezetet, a látogató aláírását, az azonosítás módját, a belépés dátumát, a belépés és a távozás időpontjait, a látogatás célját, valamint a felkeresett személyek nevét és szervezetét vagy szervezeti egységét. A hozzférési naplók felülvizsgálatával megállapítható, hogy a hozzáférési jogosultságok napra készek-e és továbbra is szükségesek-e a szervezeti alapfeladatokhoz és az üzleti funkcióhoz. Hozzáférési naplókat nem szükséges készíteni a nyilvánosan hozzáférhető területek vonatkozásában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek rögzítenie kell fizikai és környezeti védelemről szóló szabályzatában a látogatók naplózását, valamint létre kell hoznia egy eljárásrendet, amely biztosítja, hogy a szervezet nyomon követi és rögzíti a látogatók belépéseit az EIR-eknek helyt adó létesítményekbe.

2. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia a látogatói belépésekről szóló nyilvántartást. Ez a felülvizsgálat annak ellenőrzését szolgálja, hogy a hozzáférési engedélyek aktuálisak-e és továbbra is szükségesek-e az érintett szervezet célkitűzéseihez és üzleti funkcióinak támogatásához.

3. A szervezetnek azonnal jelentenie kell a látogatói belépésekről szóló nyilvántartásban észlelt rendellenességeket a meghatározott személynek vagy szerepkörnek.

4. A szervezetnek meg kell határoznia, hogy mennyi ideig őrzi meg a látogatói belépésekről szóló információkat. Ennek során az érintett szervezetnek figyelembe kell venni a jogszabályi előírásokat.

Kapcsolódó intézkedések

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

12.17. A fizikai hozzáférések felügyelete

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

3.2.1.8. A látogatók ellenőrzése

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PE-8

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.23. LÁTOGATÓI HOZZÁFÉRÉSI NAPLÓK – NYILVÁNTARTÁSOK AUTOMATIZÁLT KARBANTARTÁSA ÉS FELÜLVIZSGÁLATA

12.23. A szervezet automatizált eszközöket alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez és átvizsgálásához.

MAGYARÁZAT

A látogatói belépésekkel kapcsolatos nyilvántartásokat az érintett szervezet tárolhatja és karban is tarthatja egy olyan adatbázis-kezelő rendszerben, amelyhez a szervezet ezért felelős munkavállalói (vagy megbízott szervezethez köthető személyek) is hozzáférnek. Az említett információkhoz történő automatizált hozzáférés megkönnyíti azok rendszeres felülvizsgálatát és segít meghatározni, hogy a belépési engedélyek naprakészek-e, és továbbra is szükségesek-e a szervezeti célkitűzések és az üzleti funkciók támogatásához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie egy automatizált eszközt, amely képes kezelni és átvizsgálni a látogatói belépésekről készített információkat és felvételeket.
2. A szervezet tárolhatja és egyúttal karban is tarthatja egy adatbázis-kezelő rendszerben a látogatói hozzáférési naplókat. Az említett rendszerhez hozzá kell, hogy férjenek az érintett szervezet felelős munkavállalói vagy szerződéses megbízottak.
3. Az automatizált hozzáférés lehetővé teszi az érintett szervezet számára, hogy rendszeresen felülvizsgálja a naplókat, és ellenőrizze, hogy a hozzáférési engedélyek aktuálisak-e és továbbra is szükségesek-e az érintett szervezet célkitűzéseinek és üzleti funkcióinak támogatásához.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.2.1.8. A látogatók ellenőrzése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

PE-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

12.24. ÁRAMELLÁTÓ BERENDEZÉSEK ÉS KÁBELEZÉS

12.24. A szervezet védi az EIR áramellátását biztosító berendezéseket és a kábelezést a sérülésektől és rongálásoktól.

MAGYARÁZAT

Az érintett szervezet gondoskodik arról, hogy az EIR áramellátását biztosító berendezések és a kábelezés megfelelően védett legyen a sérülésektől és rongálásoktól. Ez magában foglalja a fizikai védelmet, mint például a kábelek burkolatának és a berendezések házának ellenálló képességét a mechanikai sérülésekkel szemben, valamint a környezeti károk elleni védelmet, mint például a víz, hő vagy por elleni védelem.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a szükséges védelmi intézkedéseket az EIR áramellátását biztosító berendezésekhez és a kábelezéshez, amelyeket a szervezeti működési környezeten belül és kívül található berendezések és kábelek vonatkozásában is alkalmaz.
2. A szervezetnek gondoskodnia kell arról, hogy az EIR áramellátását biztosító berendezések és a kábelezés megfelelően védett legyen a sérülésektől és rongálásoktól.
3. A szervezetnek rendszeresen felül kell vizsgálnia az EIR áramellátását biztosító berendezések és a kábelezés állapotát, azonosítja az esetleges sérüléseket és rongálásokat. Ez lehetővé teszi az érintett szervezet számára, hogy időben észlelje a problémákat és megfelelő intézkedéseket tegyen azok megoldására.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az EIR áramellátását biztosító berendezések és a kábelezés védelmi intézkedéseit, hogy biztosítsa azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

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

3.2.1.9. Áramellátó berendezések és kábelezés: Az érintett szervezet védi azelektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

ISO/IEC 27001:2023 REFERENCIA

A.7.5; A.7.8; A.7.11; A.7.12

NIST SP 800-53 REV.5 REFERENCIA

PE-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

12.25. Áramellátó berendezések és kábelezés – Redundáns kábelezés

12.25. A szervezet redundáns tápellátó kábelútvonalakat alkalmaz, amelyeket egymástól meghatározott távolságra helyez el.

Magyarázat

A fizikailag különálló és redundáns tápkábelek biztosítják, hogy az áramellátás akkor is folytatódjon, ha az egyik kábelt elvágják vagy más módon megsérül.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a redundáns tápkábelek útvonalait. Ez azt jelenti, hogy több, egymástól független tápkábel útvonalat kell létrehoznia az érintett szervezetnek, amelyek képesek biztosítani az EIR működését akkor is, ha az egyik kábel elvágják vagy más módon megsérül.
2. A szervezetnek fizikailag el kell különítenie a tápellátó kábeleket, így biztosítva a redundanciát. A közöttük lévő távolságnak elegendőnek kell lennie ahhoz, hogy ha az egyik kábel megsérül, a többin az áramellátás zavartalanul folytatódjon.
3. A szervezetnek gondoskodnia kell a redundáns tápkábelek útvonalainak megfelelő karbantartásáról és ellenőrzéséről. Ez magában foglalja a kábelek rendszeres átvizsgálását, illetve azok cseréjét, amennyiben szükséges.
4. A szervezetnek dokumentálnia kell a redundáns tápkábelekkel kapcsolatos karbantartásokat és ellenőrzéseket. A dokumentálás segít az érintett szervezetnek nyomon követni a kábelek állapotát, és időben észlelni a potenciális problémákat.

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

PE-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a távolság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.26. ÁRAMELLÁTÓ BERENDEZÉSEK ÉS KÁBELEZÉS – AUTOMATIKUS FESZÜLTSÉGSZABÁLYOZÁS

12.26. A szervezet automatikus feszültségszabályozót alkalmaz a meghatározott EIR és a szervezet működése szempontjából kritikus rendszerelemeknél.

MAGYARÁZAT

Az automatikus feszültségszabályozás alkalmazásával az érintett szervezet képes a feszültség felügyeletére és szabályozására. Az ilyen vezérlők közé tartoznak a feszültségszabályozók, a tápfeszültség kondicionálók és a feszültségstabilizátorok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy melyek azok az rendszerelemek, amelyek kritikusak a működés szempontjából.
2. A szervezetnek automatikus feszültségszabályozót kell alkalmaznia a kritikus rendszerelemek vonatkozásában, melyek felügyelik és szabályozzák a feszültséget.
3. A szervezetnek gondoskodnia kell arról, hogy az automatikus feszültségszabályozók megfelelően működjenek és azok szükség esetén beavatkoznak a feszültség szabályozásába.

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

PE-9(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kritikus rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.27. VÉSZKIKAPCSOLÁS

12.27. A szervezet:

12.27.1. Lehetőséget biztosít az EIR vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben.

12.27.2. Gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről az arra jogosult személyek számára.

12.27.3. Megakadályozza a jogosulatlan vészkikapcsolást.

MAGYARÁZAT

A áramellátás kikapcsolása vészhelyzetben elsősorban az érintett szervezet azon létesítményeire vonatkozik, amelyek egyszerre több informatikai erőforrást tartalmaznak, pl. adatközpontok, számítógéptermek, szerverszobák és olyan területek, melyekben számítógép által vezérelt gépek találhatók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR vagy egyedi rendszerelemek áramellátása vészhelyzet esetén kikapcsolható legyen. Ez elsősorban olyan szervezeti létesítményekre vonatkozik, amelyek koncentráltan tartalmaznak informatikai erőforrást, pl. adatközpontok, számítógéptermek, szerverszobák és olyan területek, melyekben számítógép által vezérelt gépek találhatók.

2. A szervezetnek gondoskodnia kell a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről az arra jogosult személyek számára. Ez magában foglalhatja a vészkikapcsoló berendezések megfelelő jelölését és azoknak azon helyek egyértelmű jelzését, ahol ezek a berendezések találhatók.

3. A szervezetnek meg kell akadályoznia a jogosulatlan vészkikapcsolást. Ez biztosítható úgy, hogy a vészkikapcsoló berendezéseket zárt vagy korlátozott hozzáférésű területeken helyezik el.

4. A szervezetnek dokumentálnia kell vészkikapcsolással kapcsolatos eseményeket. A dokumentáció a következő információkat tartalmazhatja: a kikapcsolás időpontja, oka és a kikapcsolást végrehajtó személy neve. Ez segít azonosítani a rendszeresen előforduló

problémákat, és lehetővé teszi a szervezet számára, hogy megtegye a szükséges lépéseket a problémák megoldása érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.40. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

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

3.2.1.10. Vészkikapcsolás

ISO/IEC 27001:2023 REFERENCIA

A.7.11

NIST SP 800-53 REV.5 REFERENCIA

PE-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

12.28. VÉSZHELYZETI TÁPELLÁTÁS

12.28. A szervezet az elsődleges áramforrás kiesése esetén, a tevékenységéhez méretezett szünetmentes áramellátást biztosít az EIR szabályos leállításához, vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.

MAGYARÁZAT

Az érintett szervezetnek szüksége van szünetmentes áramellátásra - ami egy elektromos rendszer vagy mechanizmus - amely vészhelyzet esetén áramot biztosít, amennyiben az elsődleges áramforrás kiesik. A szünetmentes áramellátást tipikusan olyan számítógépek, adatközpontok, telekommunikációs berendezések vagy más elektromos berendezések védelmére használják, ahol egy váratlan áramkimaradás sérüléseket, haláleseteket, illetve adatvesztést okozhat. Emellett egy váratlan áramkimaradás komoly zavart is okozhat az üzleti tevékenységben. A szünetmentes áramellátás különbözik a vészhelyzeti áramellátási rendszertől vagy a tartalék generátortól abban, hogy a szünetmentes áramellátás szinte azonnali védelmet nyújt a váratlan áramkimaradások ellen, azáltal, hogy az akkumulátorokban, szuperkondenzátorokban és lendkerekekben tárolt energiát biztosít. A szünetmentes áramellátó akkumulátorának kapacitása rövid ideig képes biztosítani a szükséges energiát, azonban elegendő időt biztosít egy tartalék áramforrás (pl.: tartalék generátor) beindításához vagy az EIR szabályos leállításához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR energiaigényét. Ez magában foglalja az EIR működéséhez szükséges áramellátás mértékének és időtartamának meghatározását.
2. A szervezetnek szünetmentes áramellátást kell alkalmaznia, amely képes az EIR energiaigényének kielégítésére vészhelyzet esetén. A szünetmentes áramellátásnak képesnek kell lennie azonnali energiaellátást biztosítani az elsődleges áramforrás kiesése esetén.
3. A szervezetnek biztosítania kell, hogy a szünetmentes áramellátás rendelkezik a szükséges kapacitással az EIR szabályos leállításához, vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.
4. A szervezetnek tesztelnie kell a szünetmentes áramellátást, így biztosítva annak működőképességét és megbízhatóságát. Ez magában foglalja a rendszer tesztelését különböző

terhelési szintek mellett, illetve annak tesztelését, hogy a rendszer képes-e annyi ideig energiát biztosítani, amíg az érintett szervezet átáll egy hosszabb távú tartalék áramellátásra.

5. Az érintett szervezetnek dokumentálnia kell a szünetmentes áramellátás tesztelését. Ez magában foglalja a rendszer működési adatainak, hibáinak nyomon követését.

6. Az érintett szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén karban kell tartania a szünetmentes áramellátó rendszert, hogy biztosítsa annak folyamatos működőképességét és megbízhatóságát.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

7.2. Üzletmenet-folytonossági terv

7.23. Alternatív feldolgozási helyszín

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

3.2.1.9. Áramellátó berendezések és kábelezés: Az érintett szervezet védi azelektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

ISO/IEC 27001:2023 referencia

A.7.11

NIST SP 800-53 rev.5 referencia

PE-11

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

12.29. VÉSZHELYZETI TÁPELLÁTÁS – TARTALÉK ÁRAMELLÁTÁS – MINIMÁLIS MŰKÖDÉSI KÉPESSÉG

12.29. A szervezet az elsődleges áramforrás kiesése esetén automatikus vagy manuális aktiválású hosszútávú alternatív áramellátást biztosít az EIR minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.

MAGYARÁZAT

A minimális működési szint fenntartásához szükséges alternatív áramellátás kielégíthető egy másodlagos kereskedelmi szolgáltató áram ellátásához vagy egyéb külső áramellátáshoz való csatlakozással.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határozna az EIR minimálisan elvárt működési képességét és előre definiált minimálisan elvárt működési idejét. Ez magában foglalja az EIR által fogyasztott energia mennyiségének meghatározását is.
2. A szervezetnek ki kell dolgoznia egy alternatív áramellátási tervet, amely leírja, hogyan biztosítja az EIR működését az elsődleges áramforrás kiesése esetén. Ez a terv tartalmazza a hosszútávú alternatív áramellátás forrásait és azok igénybevételének módszereit is.
3. A szervezetnek be kell szereznie és telepítenie kell a szükséges berendezéseket vagy más alternatív áramforrásokat, amelyek képesek biztosítani az EIR minimálisan elvárt működési képességét és idejét.
4. A szervezetnek tesztelnie kell az alternatív áramellátási rendszert, hogy biztosítsa annak működőképességét és megbízhatóságát. Ez magában foglalja az automatikus vagy manuális tesztelést is.
5. A szervezetnek dokumentálnia kell az alternatív áramellátási rendszer tesztelésének eredményeit és az eredmények alapján szükség esetén módosítania kell az alternatív áramellátási tervet.
6. A szervezetnek biztosítania kell, hogy a személyzet megfelelően képzett és felkészült az alternatív áramellátási rendszer használatára és karbantartására.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.2.1.9. Áramellátó berendezések és kábelezés: Az érintett szervezet védi azelektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PE-11(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

12.30. VÉSZHELYZETI TÁPELLÁTÁS – TARTALÉK ÁRAMELLÁTÁS – ÖNELLÁTÁS

12.30. A szervezet automatikusan vagy kézzel aktiválható alternatív áramellátást biztosít az EIR számára, amely:

12.30.1. önálló;

12.30.2. nem függ a hálózati áramellátástól;

12.30.3. képes fenntartani a minimálisan szükséges működési képességet vagy a teljes működési képességet az elsődleges áramforrás hosszabb ideig tartó kiesése esetén.

MAGYARÁZAT

A hosszútávú, önálló áramellátás biztosítása egy vagy több, a szervezet igényeinek megfelelő kapacitású generátor használatával biztosítható.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határozna az EIR minimálisan elvárt működési képességét és előre definiált minimálisan elvárt működési idejét. Ez magában foglalja az EIR által fogyasztott energia mennyiségének meghatározását is.

2. A szervezetnek meg kell terveznie és alkalmaznia kell egy automatikusan vagy kézzel aktiválható alternatív áramellátási rendszert, amely képes önállóan működni, és nem függ a hálózati áramellátástól. Emellett képes fenntartani a minimálisan szükséges működési képességet vagy a teljes működési képességet az elsődleges áramforrás hosszabb ideig tartó kiesése esetén.

4. A szervezetnek tesztelnie kell az alternatív áramellátási rendszert, hogy biztosítsa annak működőképességét és megbízhatóságát. Ez magában foglalja a rendszer automatikus vagy kézi aktiválásának tesztelését is.

5. A szervezetnek dokumentálnia kell az alternatív áramellátási rendszer tesztjeit és azok eredményeit, és az eredmények alapján szükség esetén módosítania kell azokat.

6. A szervezetnek biztosítania kell, hogy a személyzet megfelelően képzett és felkészült az alternatív áramellátási rendszer használatára és karbantartására.

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

PE-11(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

12.31. VÉSZVILÁGÍTÁS

12.31. A szervezet alkalmaz és karbantart egy automatikus vészvilágítási rendszert a létesítményben, amely áramszünet esetén aktiválódik, és megvilágítja a vészkijáratokat és a menekülési útvonalakat.

MAGYARÁZAT

A vészvilágítás biztosítása elsősorban az érintett szervezet azon létesítményeire vonatkozik, amelyek egyszerre több rendszererőforrást tartalmaznak, pl. adatközpontok, számítógéptermek, szerverszobák. A vészvilágítással kapcsolatos előírások az érintett szervezet vészhelyzeti tervében találhatók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a területeket, amelyek egyszerre több rendszererőforrást tartalmaznak, pl. adatközpontok, számítógéptermek, szerverszobák.
2. A szervezetnek létre kell hoznia és karban kell tartania egy automatikus vészvilágítási rendszert, amely áramszünet esetén aktiválódik, és megvilágítja a vészkijáratokat és a menekülési útvonalakat.
3. A szervezetnek tesztelnie kell az automatikus vészvilágítási rendszerét, hogy biztosítsa annak megfelelő működését áramszünet esetén.
4. A szervezetnek dokumentálnia kell az automatikus vészvilágítási rendszerének tesztelését és karbantartását, így biztosítva a rendszer megfelelő működését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.23. Alternatív feldolgozási helyszín

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

3.2.1.11. Vészvilágítás: Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

ISO/IEC 27001:2023 REFERENCIA

A.7.11

NIST SP 800-53 REV.5 REFERENCIA

PE-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

12.32. VÉSZVILÁGÍTÁS – ALAPVETŐ ÜZLETI (ÜGYMENETI) FUNKCIÓK

12.32. A szervezet biztosítja a vészvilágítást a létesítményen belül minden olyan területen, amely támogatja az üzleti funkciókat.

MAGYARÁZAT

Az érintett szervezet maga határozza meg alapvető célkitűzéseit és üzleti funkcióit.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia alapvető célkitűzéseit és üzleti funkcióit.
2. A szervezet azonosítja azokat a területeket a létesítményen belül, amelyek támogatják az üzleti funkciókat.
3. A szervezetnek biztosítania kell a vészvilágítást minden olyan területen, amely támogatja az üzleti funkciókat.
4. A szervezetnek tesztelnie kell az automatikus vészvilágítási rendszerét, hogy biztosítsa annak megfelelő működését áramszünet esetén.
5. A szervezetnek dokumentálnia kell az automatikus vészvilágítási rendszerének tesztelését és karbantartását, így biztosítva a rendszer megfelelő működését.

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

PE-12(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.33. TŰZVÉDELEM

12.33. A szervezet független energiaforrással rendelkező tűzérzékelő, illetve tűzoltó rendszereket tart fenn és alkalmaz az EIR-ek védelme érdekében.

MAGYARÁZAT

A tűzérzékelő és tűzoltó rendszerek biztosítása elsősorban az érintett szervezet azon létesítményeire vonatkozik, amelyek egyszerre több rendszererőforrást tartalmaznak, pl. adatközpontok, számítógéptermek, szerverszobák. A tűzérzékelő és tűzoltó rendszerekhez tartozó sprinkler rendszerek és füstérzékelők független energiaforrást igényelhetnek. A független energiaforrás biztosítja, hogy a tűzérzékelő és tűzoltó rendszerek akkor is működőképesek maradjanak, ha a létesítmény többi részének energiaellátása megszakad. Ez lehetővé teszi a tűz gyors észlelését és eloltását, csökkentve az EIR-ekben bekövetkező károkat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a területeket, amelyek egyszerre több rendszererőforrást tartalmaznak, pl. adatközpontok, számítógéptermek, szerverszobák.
2. A szervezet meghatározza, milyen tűzérzékelő és tűzoltó rendszerekre van szükség az EIR-ek védelme érdekében.
3. A szervezet biztosítja, hogy amennyiben szükséges a tűzérzékelő és tűzoltó rendszerek független energiaforrással rendelkezzenek.
4. A szervezetnek gondoskodnia kell arról, hogy a független energiaforrások rendelkezésre álljanak és működjenek, ha szükséges.
5. A szervezetnek biztosítania kell, hogy a tűzérzékelő és tűzoltó rendszerek megfelelően vannak telepítve és karbantartva, illetve biztosítania kell, hogy a személyzet megfelelően képzett és felkészült a tűzeset esetén megteendő intézkedések tekintetében.
6. A szervezetnek dokumentálnia kell a rendszerek tesztelését, karbantartását és az esetleges tűzeseteket is. A rendszeres teszteléssel és karbantartással biztosítható az eszközök megfelelő működése.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

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

3.2.1.12. Tűzvédelem

ISO/IEC 27001:2023 referencia

A.7.5; A.7.8

NIST SP 800-53 rev.5 referencia

PE-13

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.34. Tűzvédelem – Érzékelőrendszerek – Automatikus élesítés és értesítés

12.34. A szervezet az EIR védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld a szervezet által kijelölt tűzvédelmi felelősnek.

Magyarázat

Az érintett szervezet az EIR védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek. Ez a követelmény azt jelenti, hogy az érintett szervezetnek rendelkeznie kell egy olyan tűzjelző rendszerrel, amely képes automatikusan értesíteni a tűzvédelmi felelőst, ha tűz keletkezik. Ez a rendszer lehetővé teszi a gyors reagálást és a tűz káros hatásainak minimalizálását. A tűzjelző rendszernek független energiaforrással kell rendelkeznie, hogy tűz esetén is működőképes maradjon és értesítést küldjön a tűzvédelmi felelősnek, még akkor is, ha a tűz miatt az energiaellátás megszakad.

A követelmény alkalmazásának lépései

1. A szervezetnek gondoskodnia kell a tűzesettel kapcsolatos felelősök kinevezéséről és feladatok ellátásáról.
2. A szervezetnek olyan tűzjelző berendezést kell alkalmaznia, amely automatikusan működésbe lép tűz esetén, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelős(ök)nek
3. A szervezetnek biztosítania kell, hogy az értesítési mechanizmusok rendelkezzenek független energiaforrásokkal, hogy az értesítési képesség ne sérüljön a tűz hatására.
4. A szervezetnek dokumentálnia kell amennyiben a tűzjelző berendezés működésbe lépett.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.2.1.12. Tűzvédelem

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

PE-13(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök illetve az elsődleges beavatkozó állomány meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

12.35. TŰZVÉDELEM – TŰZOLTÓ BERENDEZÉSEK – AUTOMATIKUS ÉLESÍTÉS ÉS ÉRTESÍTÉS

12.35. A szervezet:

12.35.1. Az EIR védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld a szervezet által kijelölt tűzvédelmi felelősnek.

12.35.2. Automatikus tűzoltó berendezést alkalmaz, ha a létesítményben nincs állandó személyzet.

MAGYARÁZAT

Az érintett szervezet az EIR védelmére olyan tűzoltó berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek. Ez a követelmény azt jelenti, hogy az érintett szervezetnek rendelkeznie kell egy olyan tűzoltó rendszerrel, amely képes automatikusan értesíteni a tűzvédelmi felelőst, ha tűz keletkezik. Ez a rendszer lehetővé teszi a gyors reagálást és a tűz káros hatásainak minimalizálását. A tűzoltó rendszernek független energiaforrással kell rendelkeznie, hogy tűz esetén is működőképes maradjon és értesítést küldjön a tűzvédelmi felelősnek, még akkor is, ha a tűz miatt az energiaellátás megszakad. Ha a létesítményben nincs állandó személyzet, az érintett szervezet automatikus tűzoltó berendezést alkalmaz. Ez a berendezés automatikusan aktiválódik tűz esetén, és eloltja a tüzet, még mielőtt az komoly károkat okozhatna az EIR-ben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a tűzesettel kapcsolatos felelősségi feladatok ellátásáról.
2. A szervezetnek olyan tűzoltó berendezést kell alkalmaznia, amely automatikusan működésbe lép tűz esetén, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek.
3. A szervezetnek biztosítania kell, hogy az értesítési mechanizmusok rendelkezzenek független energiaforrásokkal, hogy az értesítési képesség ne sérüljön a tűz hatására.
4. A szervezetnek dokumentálnia kell a tűzoltó berendezés működésbe lépését.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.2.1.12. Tűzvédelem

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PE-13(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

12.36. TŰZVÉDELEM – HATÓSÁGI ELLENŐRZÉSEK

12.36. A szervezet biztosítja, hogy a létesítményt a jogszabályi előírásoknak megfelelő ellenőrök a vonatkozó jogszabályok szerint és a szervezet által meghatározott gyakorisággal tűzvédelmi ellenőrzésnek vessék alá, és az azonosított hiányosságokat a vonatkozó jogszabályok és a szervezet által meghatározott időn belül orvosolják.

MAGYARÁZAT

Az érintett szervezet telephelye szerinti illetékességi és hatáskörrel rendelkező tűzvédelmi hatóság rendszeres időnként vagy eseti jelleggel tűzvédelmi hatósági ellenőrzést tarthat, ahol a szervezet által felhatalmazott és képzett személyzet (tűzvédelmi felelős, tűzvédelmi szakértő, tűzvédelmi szolgáltató munkavállalója) is megjelenhet. A szervezetek kíséretet biztosítanak az ellenőrzések során olyan helyzetekben, amikor a létesítményekben található rendszerek érzékeny információkat tartalmaznak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a létesítményben működő tűzvédelmi rendszereit jogszabályi előírásoknak megfelelő, hozzáértő személyek rendszeresen ellenőrizzék.
2. A szervezetnek gondoskodnia kell arról, hogy az ellenőrzések során kísérők legyenek jelen, különösen, ha a rendszer bizalmas információkat tartalmaz.
3. A szervezetnek biztosítania kell, hogy a belső, valamint hatósági tűzvédelmi ellenőrzések rendszeresen, meghatározott időközönként megtörténjenek.
4. A szervezetnek biztosítania kell, hogy az ellenőrzések során azonosított hiányosságokat a vonatkozó jogszabályok és a szervezet által vagy hatóság által meghatározott időn belül orvosolják.
5. Az érintett szervezetnek dokumentálnia kell a tűzvédelmi ellenőrzéseket és az azok során azonosított hiányosságokat, valamint a hatósági ellenőrzésekről készült jegyzőkönyveket archiválniuk kell.

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

PE-13(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság illetve az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.37. KÖRNYEZETI VÉDELMI INTÉZKEDÉSEK

12.37. A szervezet:

12.37.1. Meghatározott biztonságos szinten tartja a hőmérsékletet, a páratartalmat, a légnyomást és a sugárzást az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (például: adatközpont, szerver szoba, központi gépterem).

12.37.2. Felügyeli a környezeti szabályozási szinteket a szervezet által meghatározott gyakorisággal.

MAGYARÁZAT

A környezeti feltételekhez kapcsolódó követelmények elsősorban a szervezet azon létesítményeire vonatkoznak, ahol koncentráltan találhatóak meg informatikai erőforrások. A környezeti feltételekhez kapcsolódó követelmények biztosítása elsősorban az érintett szervezet azon létesítményeire vonatkozik, amelyek egyszerre több rendszererőforrást tartalmaznak (pl.: adatközpontok, számítógéptermek, szerverszobák). A környezeti tényezők elégtelen felügyelete - különösen zord működési környezetben - negatívan befolyásolhatja a szervezet ügymeneti és üzleti funkcióinak ellátásához szükséges EIR-ek és rendszerelemek rendelkezésre állását. Az érintett szervezetnek gondoskodnia kell arról, hogy a környezeti tényezők ne lépjék túl a biztonságos határokat, mivel ebben az esetben károsíthatják a rendszererőforrásokat vagy veszélyeztethetik azok működését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonságos szinteket (tartományokat) a környezeti feltételeket illetően.

2. A szervezetnek be kell állítania a környezeti szabályozó rendszereket, hogy fenntartsa ezeket a biztonságos szinteket. Ez magában foglalhatja a klímaberendezések, páramentesítők, légnyomás szabályozók és sugárzásvédelmi eszközök használatát, illetve azok beállításait.

3. A szervezetnek rendszeresen ellenőriznie kell a környezeti szabályozási szinteket. Ez magában foglalhatja a hőmérséklet, páratartalom, légnyomás és sugárzás mérését, valamint a mérési adatok dokumentálását.

4. A szervezetnek be kell állítania automatikus riasztást, amely figyelmezteti a meghatározott személyzetet, ha a környezeti szabályozási szintek a biztonságos tartományon kívül esnek. Ez lehetővé teszi a gyors reagálást és a problémák korai megoldását.
5. A szervezetnek rendszeresen felül kell vizsgálnia a környezeti szabályozási szinteket és a riasztási rendszert, hogy biztosítsa azok hatékonyságát és naprakészségét. Szükség esetén módosítania kell ezeket.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

7.2. Üzletmenet-folytonossági terv

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

3.2.1.13. Hőmérséklet és páratartalom ellenőrzés

ISO/IEC 27001:2023 referencia

A.7.5; A.7.8; A.7.11

NIST SP 800-53 rev.5 referencia

PE-14

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

12.38. KÖRNYEZETI VÉDELMI INTÉZKEDÉSEK – AUTOMATIKUS SZABÁLYOZÁS

12.38. A szervezet automatizált környezeti szabályozó eszközöket alkalmaz a létesítményben, hogy megakadályozza azokat az ingadozásokat, amelyek potenciálisan károsak lehetnek az EIR-re nézve.

MAGYARÁZAT

Az automatikus környezeti szabályozó eszközök bevezetése azonnali választ ad az olyan környezeti körülményekre, amelyek károsíthatják vagy tönkretehetik a szervezeti rendszereket vagy EIR-t vagy annak rendszerelemeit.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, milyen környezeti ingadozások lehetnek potenciálisan károsak az EIR számára. Ez magában foglalhatja a hőmérséklet, páratartalom, vízszint, por, elektromágneses sugárzás és egyéb környezeti tényezők figyelembevételét.
2. A szervezetnek automatikus környezeti szabályozó eszközöket kell bevezetnie, amelyek képesek érzékelni és reagálni ezekre az ingadozásokra. Ez magában foglalhatja a hőmérséklet-szabályozók, páratartalom-szabályozók, vízszint-érzékelők, por-érzékelők, elektromágneses sugárzás-érzékelők és egyéb környezeti érzékelők használatát.
3. A szervezetnek biztosítania kell, hogy ezek az eszközök megfelelően vannak beállítva és karbantartva, hogy folyamatosan működjenek és megfelelően reagáljanak a környezeti ingadozásokra.
4. A szervezetnek naplóznia kell a környezeti szabályozó eszközök működését és az általuk észlelt ingadozásokat. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a környezeti feltételeket és az eszközök reakcióit, és szükség esetén módosítsa a beállításokat.

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

PE-14(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatikus környezeti szabályozók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.39. KÖRNYEZETI VÉDELMI INTÉZKEDÉSEK – FELÜGYELETI RIASZTÁSOK ÉS ÉRTESÍTÉSEK

12.39. Az adott szervezet egy olyan biztonsági rendszert használ, amely figyelmezteti a kijelölt személyeket vagy szerepeket, ha olyan változások történnek, amelyek potenciálisan veszélyeztethetik az embereket vagy a berendezéseket.

MAGYARÁZAT

A riasztás vagy értesítés lehet hangjelzés vagy vizuális üzenet valós időben a szervezet által meghatározott személyek vagy szerepek számára. Az ilyen riasztások és értesítések segíthetnek a személyi és a szervezeti eszközökben keletkezett károk minimalizálásában azáltal, hogy elősegítik az időben történő eseményre adott válaszlépéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely személyek vagy szerepek felelősek a kiberbiztonsági események kezeléséért. Ezek a személyek vagy szerepek lesznek azok, akiket az EIR figyelmeztetni fog a potenciálisan veszélyes eseményekről.
2. A szervezetnek be kell vezetnie egy rendszert, amely képes valósidejű figyelmeztetést küldeni a kijelölt személyek vagy szerepek számára. Ez lehet egy hangjelzés, szöveges üzenet vagy más típusú értesítés.
3. Az rendszernek képesnek kell lennie arra, hogy naplózza az összes potenciálisan veszélyes változást. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse és elemezze a változásokat, és megtegye a szükséges lépéseket a kockázatok kezelésére.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a rendszert, hogy biztosítsa annak hatékonyságát és relevanciáját. Ez magában foglalhatja beállítások finomhangolását, a figyelmeztetések és értesítések paramétereinek módosítását, és a naplózás gyakoriságának és részletességének beállítását.

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

PE-14(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.40. VÍZ-, ÉS MÁS, CSŐVEZETÉKEN SZÁLLÍTOTT ANYAG OKOZTA KÁR ELLENI VÉDELEM

12.40. Védi az EIR-t a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetők és működőképesek, valamint a nélkülözhetetlen szerepköröket betöltő személyek számára ismertek legyenek.

MAGYARÁZAT

A vízkár elleni védekezés elsősorban azokra a szervezeti létesítményekre vonatkozik, amelyekben rendszererőforrások koncentrálódnak, beleértve az adatközpontokat, szervertermeket és nagy teljesítményű számítógépes helyiségeket. Az elzárószelepek a főelzárószelepek mellett vagy helyett is alkalmazhatók a vízellátás elzárására az egyes problémás területeken anélkül, hogy az egész szervezetet érintené.

Az EIR védelme a csővezeték rongálódásból származó károk ellen nem csak a fizikai infrastruktúra védelmét jelenti, hanem a hozzáférhetőség és a működőképesség biztosítását is. A főelzáró szelepeknek hozzáférhetőnek és működőképesnek kell lenniük, hogy a szükséges intézkedéseket gyorsan és hatékonyan lehessen végrehajtani. Ezenkívül fontos, hogy az EIR védelmében kulcsszerepet játszó személyek tisztában legyenek a feladataikkal és felelősségeikkel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR-t vagy rendszerelemeit tartalmazó létesítményei, mint például adatközpontok, szervertermek és főszámítógép-termek, megfelelően védettek legyenek a csővezeték rongálódásból származó károk ellen.
2. A szervezetnek használnia kell az elzárószelepeket, amelyeket a főelzárószelepek mellett vagy helyett lehet alkalmazni, hogy lezárják a vízellátást a különösen veszélyeztetett területeken, anélkül, hogy az egész szervezetet érintenék.
3. A szervezetnek biztosítania kell, hogy a főelzárószelepek hozzáférhetők és működőképesek legyenek. Ez magában foglalja a szelepek karbantartását és rendszeres ellenőrzést.
4. A szervezetnek dokumentálnia kell az EIR-el kapcsolatos tevékenységeket, beleértve a vízcsövek karbantartását, a helyiséghez való hozzáférést és a változásokat. Ez lehetővé teszi a

szervezet számára, hogy nyomon kövesse és ellenőrizze az EIR állapotát, és időben észlelje a potenciális problémákat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.9. Szerepkör alapú biztonsági képzés

12.27. Vészkikapcsolás

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

3.2.1.14. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

ISO/IEC 27001:2023 REFERENCIA

A.7.5; A.7.8; A.7.11

NIST SP 800-53 REV.5 REFERENCIA

PE-15

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

12.41. VÍZ-, ÉS MÁS, CSŐVEZETÉKEN SZÁLLÍTOTT ANYAG OKOZTA KÁR ELLENI VÉDELEM – AUTOMATIZÁLÁS TÁMOGATÁSA

12.41. A szervezet automatizált mechanizmusokat alkalmaz az EIR közelében megjelenő folyadékszivárgás észlelésére, valamint a szervezet által kijelölt személyek riasztására.

MAGYARÁZAT

Az automatizált mechanizmusok közé tartoznak az értesítési rendszerek, a víz érzékelő szenzorok és a riasztók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie azokat a rendszerelemeket, amelyek segítségével folyadékérzékelésre és riasztásra automatizált mechanizmusokat alakíthat ki.
2. A szervezetnek be kell állítania a szenzorokat az EIR környezetében, ahol a folyadékszivárgás valószínűsíthető. Ez magában foglalhatja a szenzorok elhelyezését a padlón, a falakon vagy a mennyezeten, attól függően, hogy hol van a legnagyobb esély a szivárgásra.
3. A szervezetnek be kell programoznia a szenzorokat úgy, hogy automatikusan riasztást küldjenek a kijelölt személyeknek, ha folyadékszivárgást észlelnek. Ezek lehetnek automatikus SMS-ek, e-mailek vagy telefonhívások.
4. A szervezetnek tesztelnie kell a rendszert, hogy biztosítsa annak működését. Ez magában foglalhatja a folyadékszivárgás szimulálását, hogy ellenőrizze, hogy a szenzorok megfelelően érzékelik-e, és a riasztásokat megfelelően továbbítják-e.
5. Az érintett szervezetnek naplót kell vezetnie a rendszer működéséről és az esetleges riasztásokról. Ez segít azonosítani a rendszer esetleges hibáit, és lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a problémákra.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.2.1.14. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

PE-15(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

12.42. BE- ÉS KISZÁLLÍTÁS

12.42. A szervezet

12.42.1. Engedélyezi és felügyeli a szervezet által meghatározott típusú rendszerelemek létesítménybe történő beszállítását és kiszállítását a létesítményből; és

12.42.2. nyilvántartást vezet ezekről.

MAGYARÁZAT

Az érintett szervezetnek megfelelő engedélyezési eljárásokat kell bevezetnie a rendszerelemek létesítménybe történő beszállításának, ill. a létesítményből történő kiszállításának esetére. A szervezetnek felügyelni kell a be- és kiszállítási folyamatokat, és naprakész, hiteles nyilvántartást kell vezetni ezekről. A szervezetnek ki kell kényszerítenie, hogy a szervezet által bevezetett engedélyezési eljárást megkerülve, vagy annak adminisztrálását elmulasztva ne lehessen be- és kiszállítani rendszerelemeket, ezért szükség lehet a szállítási területekhez való hozzáférés korlátozására, valamint a területek elkülönítésére a EIR-ektől és a adathordozó tárolóktól.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek engedélyeznie kell és felügyelnie kell a rendszerelemek létesítménybe történő beszállítását és kiszállítását. Ez magában foglalhatja a szállítási területekhez való hozzáférés korlátozását és azok izolálását az EIR-től.
2. A szervezetnek be kell vezetnie és folyamatosan karban kell tartania egy nyilvántartási rendszert, amely nyomon követi a rendszerelemek mozgását. Ez magában foglalhatja az elemek azonosítását, a beszállítás és kiszállítás időpontját, a célállomást és a felelős személyt.
3. A szervezetnek naplót kell vezetnie minden rendszerelem mozgásáról. Ez magában foglalhatja az elem mozgásának időpontját, a célállomást, a felelős személyt és a mozgás okát.
4. A szervezetnek gondoskodnia kell róla, hogy a fenti lépéseket következetesen és szigorúan végrehajtják. Ez magában foglalhatja a szabályok betartásának ellenőrzését és a szükséges intézkedések megtételét a szabályok megsértése esetén.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.36. Rendszerelem leltár

10.2. Szabályozott karbantartás

10.4. Karbantartási eszközök

11.6. Adathordozók szállítása

12.46. Eszközök felügyelete és nyomon követése

19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

19.8. Rendszerelemek és kapcsolódó adatok eredetisége

19.16. Beszállítók értékelése és felülvizsgálata

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

3.2.1.15. Be- és kiszállítás: Az érintett szervezet engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.2; A.7.10

NIST SP 800-53 REV.5 REFERENCIA

PE-16

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

12.43. MUNKAVÉGZÉSRE KIJELÖLT ALTERNATÍV HELYSZÍN

12.43. A szervezet:

12.43.1. meghatározza és dokumentálja az alternatív munkavégzési helyeket a munkavállalók számára;

12.43.2. meghatározza a védelmi intézkedéseket az alternatív munkavégzési helyeken;

12.43.3. értékeli a védelmi intézkedések hatékonyságát az alternatív munkavégzési helyeken;

12.43.4. biztosítja a szükséges eszközöket a munkavállalók számára, hogy egy biztonsági esemény bekövetkezése esetén kommunikálni tudjanak az információbiztonságért felelős személyekkel.

MAGYARÁZAT

Az alternatív munkavégzési helyek közé tartoznak a kormányzati létesítmények vagy a munkavállalók magánlakásai. Az alternatív feldolgozóhelyektől eltérően az alternatív munkavégzési helyek könnyen elérhető alternatív helyszíneket biztosíthatnak a rendkívüli műveletek során. A szervezetek az egyes alternatív munkavégzési helyszínekre vagy helyszíntípusokra különböző védelmi intézkedéseket határozhatnak meg, a helyszíneken végzett munkával kapcsolatos tevékenységektől függően. A szervezet által meghatározott védelmi intézkedések végrehajtásának és hatékonyságának értékelése, valamint az alternatív munkavégzési helyeken bekövetkező események közlésére szolgáló eszközök biztosítása támogatja a szervezetek vészhelyzeti tervezési tevékenységét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia az alternatív munkavégzési helyeket a munkavállalók számára.

2. A szervezetnek meg kell határoznia a védelmi intézkedéseket az alternatív munkavégzési helyeken. A szervezet meghatározhat különböző intézkedési "készleteket" a specifikus alternatív munkavégzési helyekhez vagy helytípusokhoz, attól függően, hogy milyen munkával kapcsolatos tevékenységeket végeznek a helyszíneken.

3. A szervezetnek értékelnie kell a védelmi intézkedések és eljárások hatékonyságát az alternatív munkavégzési helyeken.

4. A szervezetnek biztosítania kell a szükséges eszközöket a munkavállalók számára, hogy egy biztonsági esemény bekövetkezése esetén kommunikálni tudjanak az információbiztonságért felelős személyekkel. Ez támogatja a szervezet vészhelyzeti tervezési tevékenységeit.
5. A szervezetnek dokumentálnia kell a védelmi intézkedések hatékonyságának értékelését és a biztonsági eseményeket, hogy folyamatosan javíthassa az EIR és a szervezet biztonságát.

Kapcsolódó intézkedések

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

7.23. Alternatív feldolgozási helyszín

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.14; A.6.7; A.7.9

NIST SP 800-53 rev.5 referencia

PE-17

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

12.44. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER ELEMEINEK ELHELYEZÉSE

12.44. A szervezet úgy helyezi el az EIR elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt, valamint a jogosulatlan hozzáférés lehetőségét.

MAGYARÁZAT

A fizikai és környezeti veszélyek közé tartoznak az árvizek, tüzek, tornádók, földrengések, hurrikánok, terrorizmus, vandalizmus, elektromágneses impulzus, elektromos interferencia és a beérkező elektromágneses sugárzás egyéb formái. Az érintett szervezetek figyelembe veszik a belépési pontok helyét, ahol illetéktelen személyek, bár nem kapnak hozzáférést, mégis az EIR-ek közelében tartózkodhatnak. Az ilyen közelség növelheti a szervezeti kommunikációhoz való jogosulatlan hozzáférés kockázatát vezeték nélküli csomagolvasók vagy mikrofonok segítségével, vagy az információk jogosulatlan felfedésének kockázatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fizikai és környezeti veszélyeket, amelyek befolyásolhatják a rendszerelemeit, melyek lehetnek természeti - vagy civilizációs eredetűek.
2. A szervezet meg kell terveznie és implementálnia kell a rendszerelemeinek elhelyezését úgy, hogy minimalizálja a veszélyekből adódó lehetséges károkat. Ez magában foglalhatja a rendszerelemeinek elhelyezését magasabb szinteken az áradások elleni védelem érdekében, vagy tűzálló anyagok használatát a rendszerelemeinek védelmében.
3. A szervezetnek figyelembe kell vennie a rendszerelemeinek elhelyezését a jogosulatlan hozzáférés szempontjából is. Ez magában foglalhatja a belépési pontok helyének megfontolását, ahol a jogosulatlan személyek, az EIR-ekhez nem képesek távolról sem hozzáférni azok közelsége miatt, például vezeték nélküli csomag-figyelők vagy mikrofonok használatával.
4. A szervezetnek a kockázatelemzés felülvizsgálatakor különös figyelmet kell fordítania a fizikai és környezeti veszélyek felülvizsgálatára vagy azok kiegészítésére a változó körülményeknek megfelelően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

12.15. A kimeneti eszközök hozzáférés-ellenőrzése

12.45. Információszivárgás

12.46. Eszközök felügyelete és nyomon követése

15.4. Kockázatértékelés

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

3.2.1.16. Az elektronikus információs rendszer elemeinek elhelyezése: Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.5; A.7.8

NIST SP 800-53 REV.5 REFERENCIA

PE-18

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a fizikai és környezeti veszélyek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

12.45. INFORMÁCIÓSZIVÁRGÁS

12.45. A szervezet megvédi az EIR-t az elektromágneses jelek kisugárzása miatt bekövetkező információszivárgástól.

MAGYARÁZAT

Az információszivárgás az adatok vagy információk szándékos vagy véletlen kiszivárgása egy nem megbízható környezetbe az elektromágneses jelek kisugárzásából eredően. Az EIR-ek biztonsági kategóriái vagy besorolása, a szervezeti biztonsági szabályok és a kockázattűrés irányítják az EIR-ek elektromágneses jeleinek kisugárzása miatti információszivárgás elleni védelemre alkalmazott ellenintézkedések kiválasztását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR biztonsági kategóriáit vagy osztályozásait a titkosság szempontjából. Ez segít meghatározni, milyen adatokat kell védeni az elektromágneses jelek kisugárzása miatt bekövetkező információszivárgástól.
2. A szervezetnek ki kell dolgoznia egy szervezeti biztonsági szabályzatot vagy eljárást, amely meghatározza, hogyan kell kezelni és védeni az EIR-t az információszivárgás ellen.
3. A szervezetnek meg kell határoznia a kockázati toleranciát a védelmi szint meghatározása és kialakítása miatt, azaz mennyi kockázatot hajlandó vállalni az EIR-el kapcsolatban.
4. A szervezetnek ki kell választania és alkalmaznia kell a megfelelő védelmi intézkedéseket, hogy megvédje az EIR-t az elektromágneses jelek kisugárzása miatt bekövetkező információszivárgástól. Ez magában foglalhatja az EIR fizikai elhelyezkedésének megváltoztatását, az elektromágneses sugárzást blokkoló anyagok használatát, vagy a sugárzást kibocsátó eszközök korlátozását.
5. A szervezetnek dokumentálnia kell az összes védelmi intézkedést és követelményt, amelyet az EIR védelme érdekében hoztak. Ez segít nyomon követni, hogy mely intézkedések voltak hatékonyak, és lehetővé teszi a folyamatok folyamatos javítását.

Kapcsolódó intézkedések

2.108. Vezeték nélküli hozzáférés

12.44. Az információs rendszer elemeinek elhelyezése

12.46. Eszközök felügyelete és nyomon követése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.7.5; A.7.8; A.8.12

NIST SP 800-53 rev.5 referencia

PE-19

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

12.46. ESZKÖZÖK FELÜGYELETE ÉS NYOMON KÖVETÉSE

12.46. A szervezet olyan technológiákat alkalmaz, amelyek képesek a szervezet által meghatározott eszközök helyének és mozgásának nyomon követésére a szervezet által ellenőrzött területeken belül.

MAGYARÁZAT

Az eszközök helymeghatározási technológiái segíthetnek biztosítani, hogy a kritikus eszközök - beleértve a járműveket, berendezéseket és rendszerelemeket - az engedélyezett helyeken maradjanak. A szervezetek konzultálnak az adatvédelmi felelőssel és a jogi osztállyal az eszközhelymeghatározási technológiák telepítésével és használatával kapcsolatban, hogy kezeljék az esetleges adatvédelmi aggályokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely eszközöket kívánja nyomon követni. Ezek lehetnek járművek, berendezések, vagy a rendszerelemek.
2. A szervezetnek ki kell választania és be kell szereznie azokat a technológiákat, amelyek képesek az eszközök helyének és mozgásának nyomon követésére. Ez lehet például GPS nyomkövető, RFID technológia, vagy Wi-Fi alapú nyomkövetés.
3. A szervezetnek be kell vezetnie a nyomkövető technológiát az EIR-be, és integrálnia kell azt a meglévő rendszerekkel és folyamatokkal.
4. A szervezetnek konzultálnia kell az adatvédelmi felelőssel és / vagy a jogi osztállyal a nyomkövető technológiák telepítésével és használatával kapcsolatos esetleges adatvédelmi aggályok kezelése érdekében.
5. A szervezetnek naplóznia kell az eszközök helyét és mozgását, és rendszeresen felül kell vizsgálnia a naplókat, hogy biztosítsa az eszközök megfelelő helyen tartózkodnak.
7. A szervezetnek folyamatosan frissítenie és karbantartania kell a nyomkövető technológiát, hogy biztosítsa annak hatékony működését és a szervezet kiberbiztonsági követelményeinek való megfelelést.

Kapcsolódó intézkedések

6.36. Rendszerelem leltár

12.42. Be- és kiszállítás

1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.10

NIST SP 800-53 rev.5 referencia

PE-20

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az eszközök helyének nyomonkövetésére szolgáló technológiák illetve az eszközök meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

12.47. ELEKTROMÁGNESES IMPULZUS ELLENI VÉDELEM

12.47. A szervezet meghatározott védelmi intézkedéseket alkalmaz az EIR-ek és rendszerelemek védelmére az elektromágneses impulzusok okozta károk ellen.

MAGYARÁZAT

Az elektromágneses impulzus egy rövid, több frekvencián terjedő elektromágneses energiahullám. Az ilyen energiakitörés lehet természetes vagy ember által okozott. Az EMP interferencia zavaró vagy károsíthatja az elektronikus berendezéseket. Az EMP kockázatának csökkentésére alkalmazott védelmi intézkedések közé tartozik az árnyékolás, a túlfeszültség-csökkentők, a ferrorezonáns transzformátorok és a földelés. Az EMP-védelem különösen fontos lehet a kritikus infrastruktúrának részét képező EIR-ek és alkalmazások esetében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie az EIR-ek és rendszerelemek elektromágneses impulzusokkal szembeni sebezhetőségét.
2. A szervezetnek meg kell határoznia a megfelelő védelmi intézkedéseket, amelyeket az EIR-ek és rendszerelemek elektromágneses impulzusok okozta károk ellen alkalmazni kell. Ezek az intézkedések magukban foglalhatják a pajzsolást, a túlfeszültség-védőket, a ferrorezonáns transzformátorokat és a földelést.
3. A szervezetnek implementálnia kell a kiválasztott védelmi intézkedéseket. Ez magában foglalhatja a megfelelő berendezések beszerzését és telepítését, valamint a személyzet képzését az intézkedések megfelelő alkalmazásával kapcsolatban.
4. A szervezetnek rendszeresen dokumentálnia kell a védelmi intézkedések hatékonyságát. Ez magában foglalhatja a tesztelést és a monitorozást, hogy biztosítsák az intézkedések megfelelő működését és hatékonyságát.
5. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell az EMP elleni védelmi intézkedéseket, hogy biztosítsa az EIR-ek és rendszerelemek megfelelő védelmét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

12.44. Az információs rendszer elemeinek elhelyezése

12.45. Információszivárgás

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

PE-21

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a védelmi intézkedések, illetve a rendszer és rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

12.48. RENDSZERELEMEK JELÖLÉSE

12.48. A szervezet kijelöli az EIR-ben azokat a hardverelemeket, amelyek képesek meghatározott biztonsági besorolású információkat feldolgozni, tárolni és továbbítani.

MAGYARÁZAT

A jelölést igénylő hardverelemek közé tartoznak a bemeneti és kimeneti eszközök. A beviteli eszközök közé tartoznak az asztali és notebook számítógépek, billentyűzetek, táblagépek és okostelefonok. A kimeneti eszközök közé tartoznak a nyomtatók, monitorok/videokijelzők, telefaxok, szkennerek, fénymásolók és hangeszközök. Az alkatrészeket úgy jelölik, hogy jelzik annak a rendszernek a hatásszintjét vagy minősítési szintjét, amelyhez az eszközök csatlakoznak, illetve a kimenetre engedélyezett információk hatásszintjét vagy minősítési szintjét. A biztonsági jelölés az ember által olvasható biztonsági tulajdonságok használatára utal. A biztonsági címkézés a rendszer belső adatstruktúráira vonatkozó biztonsági tulajdonságok használatára utal. A biztonsági jelölés általában nem szükséges az olyan hardverelemek esetében, amelyek a szervezetek által "közkincsnek" vagy nyilvánosan kiadhatónak minősített információkat dolgoznak fel, tárolnak vagy továbbítanak. A szervezetek azonban megkövetelhetik a jelöléseket a nyilvános információkat feldolgozó, tároló vagy továbbító hardverelemek esetében annak jelzésére, hogy az ilyen információk nyilvánosan kiadhatók. A rendszer hardverelemek jelölése tükrözi az alkalmazandó törvényeket, végrehajtási utasításokat, irányelveket, szabályokat, szabályozásokat és szabványokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a hardverelemeket az EIR-ben, amelyek képesek meghatározott biztonsági besorolású információkat feldolgozni, tárolni és továbbítani.
2. A szervezetnek engedélyeket kell beállítania, amelyek szabályozzák a kimeneti eszközökre történő kimenetet. Ezeket az engedélyeket a "Hozzáférés-ellenőrzés érvényesítése (Hozzáférés-felügyelet)" vagy "Információáramlási szabályok érvényesítése (Hozzáférés-felügyelet)" szabályozásokban találhatóak.
3. A szervezetnek meg kell jelölnie a hardverelemeket, hogy jelezze az EIR hatásszintjét vagy besorolási szintjét, amelyhez az eszközök csatlakoznak, vagy az információ hatásszintjét vagy besorolási szintjét, amelyek kimenetelére engedélyezett.

4. A szervezetnek biztonsági jelöléseket kell alkalmaznia, amelyek ember által olvasható biztonsági tulajdonságokat használnak.
5. A szervezetnek nem szükséges biztonsági jelölést alkalmaznia azokra a hardverelemekre, amelyek olyan információkat dolgoznak fel, tárolnak vagy továbbítanak, amelyeket az érintett szervezet a nyilvános domainhez tartozónak vagy nyilvánosan kiadhatónak határoz meg. Azonban az érintett szervezet megkövetelheti a jelöléseket azokra a hardverelemekre, amelyek nyilvános információkat dolgoznak fel, tárolnak vagy továbbítanak, hogy jelezzék, hogy az ilyen információk nyilvánosan kiadhatók.
6. A szervezetnek dokumentálnia kell a fent említett lépéseket, hogy bizonyíthassa a kiberbiztonsági követelményeknek való megfelelést.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
2.28. Információáramlási szabályok érvényesítése
2.89. Biztonsági tulajdonságok
11.3. Adathordozók címkézése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.13

NIST SP 800-53 rev.5 referencia

PE-22

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszer hardverelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

12.49. LÉTESÍTMÉNY ELHELYEZKEDÉSE

12.49. A szervezet:

12.49.1. Figyelembe veszi a fizikai és környezeti veszélyeket az EIR-nek helyet adó létesítmény megtervezésekor.

12.49.2. A meglévő létesítményeknél figyelembe veszi a szervezeti kockázatmenedzsment stratégiában szereplő fizikai és környezeti veszélyeket.

MAGYARÁZAT

A fizikai és környezeti veszélyek közé tartoznak az árvizek, tüzek, tornádók, földrengések, hurrikánok, terrorizmus, vandalizmus, elektromágneses impulzus, elektromos interferencia és a beérkező elektromágneses sugárzás egyéb formái.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fizikai és környezeti veszélyeket, amelyek befolyásolhatják az EIR-t.
2. A szervezetnek figyelembe kell vennie ezeket a veszélyeket az EIR-t helyt adó létesítmény megtervezésekor. Ez magában foglalja az EIR rendszerelemeinek helyét a létesítményen belül.
3. A már meglévő létesítmények esetében a szervezetnek figyelembe kell vennie a szervezeti kockázatkezelési stratégiában szereplő fizikai és környezeti veszélyeket.
4. A szervezetnek rendszeresen dokumentálnia kell és felül kell vizsgálnia a fizikai és környezeti veszélyeket, hogy nyomon követhesse a kockázatok változásait és időben reagálhasson rájuk.
5. A szervezetnek a veszélyek felülvizsgálatából származó eredményeket be kell építenie a kockázatkezelési stratégiájába, hogy biztosítsa az EIR védelmét az aktuális fizikai és környezeti veszélyekkel szemben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

12.44. Az információs rendszer elemeinek elhelyezése

12.45. Információszivárgás

1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

1.10. Kockázatkezelési stratégia

15.4. Kockázatértékelés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.7.5; A.7.8

NIST SP 800-53 REV.5 REFERENCIA

PE-23

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024