Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Adathordozók védelme

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

11.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

11.1. A szervezet:

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

11.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó adathordozók védelmére vonatkozó szabályzatot, amely

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

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

11.1.1.2. az adathordozók védelmére vonatkozó eljárásrendet, amely az adathordozók védelmére vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

11.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az adathordozók védelmére vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

11.1.3. Felülvizsgálja és frissíti az aktuális, adathordozók védelmére vonatkozó szabályzatot és az adathordozók védelmére vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

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

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

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

által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

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

3.3.8.1. Adathordozók védelmére vonatkozó 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

MP-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

11.2. HOZZÁFÉRÉS AZ ADATHORDOZÓKHOZ

11.2. A szervezet korlátozza a hozzáférést a meghatározott digitális vagy analóg adathordozókhoz, és ezt a hozzáférést kizárólag a szervezet által meghatározott személyek vagy szerepkörök számára engedélyezi.

MAGYARÁZAT

Az EIR adathordozói lehetnek digitális és analóg adathordozók. Digitális adathordozók alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely digitális és analóg adathordozókhoz kívánja korlátozni a hozzáférést.
2. A szervezetnek meg kell határoznia azokat a személyeket vagy szerepköröket, akik számára engedélyezni kívánja a hozzáférést az említett adathordozókhoz.
3. A szervezetnek alkalmaznia kell a megfelelő hozzáférési szabályokat és eljárásrendeket, így biztosítva a hozzáférés korlátozását a meghatározott adathordozókhoz.
4. A szervezetnek dokumentálnia kell a kiosztott hozzáférési jogosultságokat, illetve azok változásait, így nyomon követheti és ellenőrizheti azokat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a hozzáférési jogosultságokat annak érdekében, hogy biztosítsa azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.113. Mobil eszközök hozzáférés-ellenőrzése
4.25. Naplóinformációk védelme
7.2. Üzletmenet-folytonossági terv
7.35. Az elektronikus információs rendszer mentései
7.43. Az elektronikus információs rendszer helyreállítása és újraindítása
10.18. Karbantartó személyek

11.4. Adathordozók tárolása

11.8. Adathordozók törlése

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

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

3.3.8.2. Hozzáférés az adathordozókhoz: Az érintett szervezet az egyesadathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.7; A.7.10

NIST SP 800-53 REV.5 REFERENCIA

MP-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a digitális vagy nem digitális adathordozó illetve a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

11.3. ADATHORDOZÓK CÍMKÉZÉSE

11.3. A szervezet:

11.3.1. Megjelöli az EIR adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket.

11.3.2. Mentesíti a meghatározott adathordozótípusokat a jelölési kötelezettség alól, ha az adathordozók a szervezet által meghatározott ellenőrzött területeken belül maradnak.

MAGYARÁZAT

A biztonsági címkézés az ember által olvasható jelölés alkalmazását jelenti. A biztonsági címkézés a biztonsági attribútumok használatát jelenti tekintettel az EIR-ben tárolt információ biztonsági szintjére. Digitális adathordozó alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm. A nyilvános adatokat tartalmazó adathordozók biztonsági címkézése általában nem szükséges. Egyes szervezetek azonban megkövetelhetik a nyilvános információk jelölését, jelezve, hogy az információ korlátozás nélkül kiadható. Az adathordozók címkézésének meg kell felelnie a szervezetre vonatkozó, hatályos jogszabályoknak, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell jelölnie az EIR adathordozóit. Emellett jeleznie kell az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket.
2. A szervezetnek mentesítenie kell a meghatározott adathordozó típusokat a jelölési kötelezettség alól, ha az adathordozók az érintett szervezet által meghatározott ellenőrzött területeken belül maradnak.
3. A szervezetnek figyelembe kell vennie a vonatkozó, hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat.

Kapcsolódó intézkedések

2.89. Biztonsági tulajdonságok

7.35. Az elektronikus információs rendszer mentései

11.6. Adathordozók szállítása

12.48. Rendszerelemek jelölése

18.67. Információ kezelése és megőrzése

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

3.3.8.3. Adathordozók címkézése: Az érintett szervezet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.

ISO/IEC 27001:2023 referencia

A.5.13

NIST SP 800-53 rev.5 referencia

MP-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

11.4. ADATHORDOZÓK TÁROLÁSA

11.4. A szervezet:

11.4.1. Fizikailag ellenőrzi és biztonságosan tárolja mind a digitális, mind az analóg adathordozókat az arra engedélyezett vagy kijelölt helyen.

11.4.2. Védi az EIR adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy a rajtuk tárolt adatot biztonságosan nem törlik.

MAGYARÁZAT

Az EIR adathordozói lehetnek digitális és analóg adathordozók. Digitális adathordozók alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm. Az EIR adathordozóinak fizikai ellenőrzése magában foglalja például az adathordozók nyilvántartását, emellett olyan eljárások biztosítását, amelyek lehetővé teszik a személyek számára, hogy a készletből elszámoltatható módon vegyék ki, illetve juttassák vissza az adathordozókat. A biztonságos tárolás történhet például zárható fiók, íróasztal vagy szekrény használatával. Az ellenőrzött területek olyan helységek, illetve terek, melyekben az információ és/vagy az EIR védelme a megfelelő fizikai és szabályozási környezet segítésével biztosított. Az adathordozók tárolására alkalmazott védelmi intézkedéseknek arányosaknak kell lenniük az adathordozókon tárolt információk biztonsági besorolásával. Az olyan adathordozók esetében, amelyeken a tárolt adatokat az érintett szervezet publikus minősítéssel látott el vagy a nyilvánosság számára elérhetőek, vagy nincsenek káros hatással a szervezetre, illetve jogosultsággal nem rendelkező személy is hozzáférhet, kevesebb biztonsági intézkedés is megfelelő lehet. Ilyen helyzetekben a fizikai hozzáféréssel kapcsolatos biztonsági intézkedések megfelelő védelmet nyújtanak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fizikailag ellenőriznie kell és biztonságosan kell tárolnia mind a digitális, mind az analóg adathordozókat az arra engedélyezett vagy kijelölt helyen.

2. A szervezet védi az EIR adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy a rajtuk tárolt adatot

biztonságosan nem törlik. Ez magában foglalja a megfelelő törlési és megsemmisítési eljárások kialakítását és alkalmazását, valamint annak dokumentálását, így nyomon követhető, hogy mely adathordozóról töröltek adatokat, illetve mely adathordozókat semmisítették meg.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.113. Mobil eszközök hozzáférés-ellenőrzése

7.2. Üzletmenet-folytonossági terv

7.19. Biztonsági tárolási helyszín

7.35. Az elektronikus információs rendszer mentései

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

11.2. Hozzáférés az adathordozókhoz

11.14. Adathordozók használata

12.6. A fizikai belépés ellenőrzése

13.2. Rendszerbiztonsági terv

17.49. Kriptográfiai kulcs előállítása és kezelése

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

3.3.8.4. Adathordozók tárolása

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.7; A.7.10; A.8.10

NIST SP 800-53 REV.5 REFERENCIA

MP-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

11.5. ADATHORDOZÓK TÁROLÁSA – AUTOMATIZÁLT KORLÁTOZOTT HOZZÁFÉRÉS

11.5. A szervezet korlátozza a hozzáférést az adathordozókat tároló ellenőrzött területekhez, valamint a szervezet által meghatározott automatizált mechanizmusok segítségével naplózza a hozzáféréseket és a hozzáférési kísérleteket.

MAGYARÁZAT

Az adathordozókat tároló ellenőrzött területek külső bejáratainál az automatizált korlátozott hozzáférést biztosítani lehet tasztatúra, biometrikus beléptető, kártyaolvasó használatával.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek korlátoznia kell a hozzáférést az adathordozókat tároló ellenőrzött területekhez. A korlátozás érvényesíthető fizikai korlátozások bevezetésével pl.: zárható ajtók, biztonsági kamerák, vagy akár biztonsági őrök alkalmazása.
2. A szervezetnek automatizált megoldásokat kell alkalmaznia a hozzáférés korlátozására pl.: tasztatúra (keypad), biometrikus beléptető, kártyaolvasó. Ezeket az érintett szervezet az adathordozókat tároló ellenőrzött területek külső bejáratainál helyezi el.
3. A szervezetnek meghatározott automatizált mechanizmusok segítségével naplóznia kell a hozzáféréseket és a hozzáférési kísérleteket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
4.2. Naplózható események
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
4.25. Naplóinformációk védelme
4.40. Naplóbejegyzések létrehozása
12.6. A fizikai belépés ellenőrzése

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

MP-4(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

11.6. ADATHORDOZÓK SZÁLLÍTÁSA

11.6. A szervezet:

11.6.1. A szervezet által meghatározott védelmi intézkedéssel védi és ellenőrzi az adathordozókat az ellenőrzött területen kívülre történő szállítás alatt.

11.6.2. Biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás alatt.

11.6.3. Dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket.

11.6.4. A jogosult személyekre korlátozza az adathordozók szállításával kapcsolatos tevékenységeket.

MAGYARÁZAT

Az EIR adathordozói lehetnek digitális és analóg adathordozók. Digitális adathordozók alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm. Ezen követelmény szabályait abban az esetben is alkalmazni kell, amennyiben valamilyen mobil eszköz rendelkezik adattárolási lehetőséggel p.: okostelefonok, tabletek, e-könyv olvasók. Illetve akkor is, amennyiben az említett eszköz kikerül a szervezet által ellenőrzött területről. Az ellenőrzött területek olyan helységek, illetve terek, melyekben az információ és/vagy az EIR védelme a megfelelő fizikai és szabályozási környezet segítésével biztosított. Az adathordozóra vonatkozó fizikai és technikai védelmi intézkedéseknek arányosnak kell lenniük az adathordozón található információk biztonsági besorolásával. Szállítás közben az adathordozó védelmét például biztosíthatják titkosítással, illetve zárható tárolóval. Az alkalmazott kriptográfiai eljárás az adatok bizalmasságát és sértetlenségét biztosítja. A szállítással kapcsolatos tevékenységek alatt a szállításra történő előkészítést, a szállító részére történő átadást, annak ellenőrzését, hogy a megfelelő szállítási folyamat kerül alkalmazásra, illetve a tényleges szállítást értjük. A szállításra jogosultak között lehetnek a szervezet oldaláról nézve külsős személyek is. Az adathordozó szállítása során az elszámoltathatóság fenntartása érdekében például az alábbi intézkedések hozhatóak: a szállítás korlátozása az arra jogosult személyekre, a szállítási tevékenységek nyomon követése és/vagy hozzáférés a szállítási folyamat tevékenységeire vonatkozó konkrét feljegyzésekhez. Mindezek alkalmazásával megelőzhető és azonosítható az adatok elvesztése, megsemmisülése vagy

manipulálása. A szervezetek dokumentációs követelményeket határoznak meg az adathordozók szállításával kapcsolatban, figyelembe véve a szervezet kockázatértékelését, és olyan rugalmas módszert határoznak meg, mely egy átfogó szállítási nyilvántartás részeként képes különböző adathordozó típusok egyedi szállítási nyilvántartásainak kezelésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a digitális és analóg adathordozókat megfelelő biztonsági intézkedésekkel védje és ellenőrizze az ellenőrzött területen kívülre történő szállítás alatt. Digitális adathordozók alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm.
2. A szervezetnek biztosítania kell az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás alatt. Ez magában foglalhatja a szállítási tevékenységek korlátozását az arra jogosult személyekre, valamint a szállítási tevékenységek nyomon követését.
3. A szervezetnek dokumentálnia kell az adathordozók szállításával kapcsolatos tevékenységeket. Az érintett szervezetnek rugalmasan kell meghatároznia a különböző típusú adathordozók szállításával kapcsolatos nyilvántartások módszereit, az EIR kockázatértékelése alapján.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.71. Sikertelen bejelentkezési kísérletek
2.113. Mobil eszközök hozzáférés-ellenőrzése
7.2. Üzletmenet-folytonossági terv
7.35. Az elektronikus információs rendszer mentései
11.3. Adathordozók címkézése
11.4. Adathordozók tárolása
12.42. Be- és kiszállítás
13.2. Rendszerbiztonsági terv
17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem

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

3.3.8.5. Adathordozók szállítása

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.9; A.7.10

NIST SP 800-53 REV.5 REFERENCIA

MP-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

11.7. ADATHORDOZÓK SZÁLLÍTÁSA – KIJELÖLT FELELŐS

11.7. A szervezet egy felügyeleti feladattal megbízott személyt jelöl ki az adathordozók ellenőrzött területeken kívüli szállítása során.

MAGYARÁZAT

Az érintett szervezetben felügyeleti feladattal megbízott személyek kapcsolattartóként funkcionálnak az adathordozók szállítási folyamata során, és elősegítik az egyéni felelősségvállalást. A felügyeleti felelősségek átadhatók egy másik személynek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell olyan személyeket, akik az adathordozók ellenőrzött területeken kívüli szállítása során felügyeleti feladatokat látnak el.
2. A felügyeleti feladattal megbízott személynek tisztában kell lennie azzal, hogy milyen adatokat tartalmaznak az adathordozók, és milyen biztonsági intézkedéseket kell betartania a szállítás során.
3. A szervezetnek biztosítania kell, hogy a felügyeleti feladattal megbízott személy rendelkezik a szükséges eszközökkel az adathordozók biztonságos szállításához.
4. A szervezetnek dokumentálnia kell vezetnie az adathordozók szállítását.
5. A szervezetnek fel kell készülnie arra, hogy a felügyeleti feladattal megbízott személy felelőssége átadható legyen egy másik személynek, amennyiben szükséges.
6. A szervezetnek biztosítania kell, hogy a felügyeleti feladattal megbízott személy rendelkezik a szükséges jogosultságokkal az adathordozó szállításához.

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

MP-5(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

11.8. ADATHORDOZÓK TÖRLÉSE

11.8. A szervezet:

11.8.1. A meghatározott, biztonságos törlési technikákkal és eljárásokkal törli az EIR meghatározott adathordozóit a leselejtezés, a szervezet ellenőrzési körén kívülre kerülés, vagy az újra felhasználásra való kibocsátás előtt.

11.8.2. A törlési mechanizmusokat az információ biztonsági besorolásával és sértetlenségi követelményével arányosan választja ki és alkalmazza.

MAGYARÁZAT

Ez a követelmény alkalmazandó minden adathordozó - legyen az digitális vagy analóg - megsemmisítésére vagy újrahasznosítására, még a hordozható adathordozókra is. Digitális adathordozó lehet szkenner, nyomtató, laptop, munkaállomás, hálózati- és hordozható eszköz. A biztonságos törlési eljárás eltávolítja az adathordozóról az információt oly módon, hogy azt nem lehet visszaállítani. A törlési eljárások megakadályozzák hogy az információt arra nem jogosult személyek megismerjék, amennyiben az adathordozót újra felhasználják vagy az kikerül a szervezet irányítása alól. A szervezet meghatározza a megfelelő törlési módszereket, melynek során figyelembe veszi, hogy a fizikai megsemmisítés szükséges lehet, amennyiben más módszerek alkalmazása nem szolgálna az elérni kívánt eredménnyel. A szervezet nem feltétlenül kell, hogy a jóváhagyott megsemmisítési technikákat és eljárásokat alkalmazza olyan esetekben, amikor az adathordozó olyan információkat tartalmaz, amelyek nyilvánosan hozzáférhetőnek minősülnek, vagy amelyek nyilvánosan közzétehetőek. Az analóg adathordozók biztonságos törlése magában foglalja például egy minősített melléklet eltávolítását egy egyébként nem minősített dokumentumból, vagy a kiválasztott szakaszok, illetve szavak olvashatatlanná tételét úgy, hogy maszkolják vagy eltávolítják a módosított részeket/szavakat. A biztonságos törlésnél, illetve megsemmisítésnél nemzetközi ajánlások figyelembevétele javasolt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek minden meghatározott digitális és analóg EIR adathordozót biztonságos törlési technikákkal és eljárásokkal törölnie kell a leselejtezés, a szervezet ellenőrzési körén kívülre kerülés, vagy az újra felhasználásra való kibocsátás előtt.
2. A szervezetnek a törlési mechanizmusokat az információ biztonsági besorolásával és sértetlenségi követelményével arányosan kell kiválasztania és alkalmaznia. A törlési eljárásnak vagy technikának úgy kell eltávolítania az információt az adathordozóról, hogy az információt ne lehessen visszaállítani.
3. A szervezetnek mérlegelnie kell, hogy a jóváhagyott megsemmisítési technikákat és eljárásokat alkalmazza-e olyan esetekben, amikor az adathordozó olyan információkat tartalmaz, amelyek nyilvánosan hozzáférhetőnek minősülnek, vagy amelyek nyilvánosan közzé tehetőek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.71. Sikertelen bejelentkezési kísérletek
4.38. A naplóbejegyzések megőrzése
10.2. Szabályozott karbantartás
10.4. Karbantartási eszközök
10.11. Távoli karbantartás
10.18. Karbantartó személyek
18.67. Információ kezelése és megőrzése

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

3.3.8.6. Adathordozók törlése

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.10; A.7.14; A.8.10

NIST SP 800-53 REV.5 REFERENCIA

MP-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

11.9. ADATHORDOZÓK TÖRLÉSE – FELÜLVIZSGÁLAT, JÓVÁHAGYÁS, NYOMON KÖVETÉS, DOKUMENTÁLÁS ÉS ELLENŐRZÉS

11.9. A szervezet felülvizsgálja, jóváhagyja, nyomonköveti, dokumentálja és ellenőrzi az adathordozók biztonságos törlésével és megsemmisítésével kapcsolatos tevékenységeket.

MAGYARÁZAT

Az érintett szervezet felülvizsgálja és jóváhagyja a törlendő adathordozókat, így biztosítja az adatok megőrzésére vonatkozó szabályzatoknak történő megfelelést. A nyomon követési/dokumentálási tevékenységek közé tartozik a személyek nyilvántartása, akik felülvizsgálták és jóváhagyták a biztonságos törlési vagy megsemmisítési intézkedéseket, a megsemmisített adathordozók típusai az adathordozón tárolt adatok, az alkalmazott törlési eljárások, a törlési vagy megsemmisítési intézkedések dátuma és időpontja, a törlést vagy megsemmisítést végző személyek, a végrehajtott ellenőrzési műveletek, az ellenőrzést végző személyek és a biztonságos törlésre vagy megsemmisítésre vonatkozó intézkedések. A szervezet meggyőződik arról, hogy az adathordozó biztonságos törlése vagy megsemmisítése sikeres volt a selejtezést megelőzően.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek felül kell vizsgálnia és jóvá kell hagynia a törlendő adathordozókat, így biztosítva az adatok megőrzésére vonatkozó szabályzatoknak történő megfelelést.
2. A szervezetnek nyomon kell követnie és dokumentálnia az adathordozók biztonságos törlésével és megsemmisítésével kapcsolatos tevékenységeket.
3. A szervezetnek meg kell győződnie arról, hogy az adathordozó biztonságos törlése vagy megsemmisítése sikeres volt a selejtezést megelőzően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.8.6. Adathordozók törlése

ISO/IEC 27001:2023 REFERENCIA

A.8.10

NIST SP 800-53 REV.5 REFERENCIA

MP-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

11.10. ADATHORDOZÓK TÖRLÉSE – BERENDEZÉS TESZTELÉSE

11.10. A szervezet a biztonságos törléshez alkalmazott eszközöket és eljárásokat a szervezet által meghatározott időközönként teszteli.

MAGYARÁZAT

A biztonságos törlésre és megsemmisítésre használt berendezések és eljárások tesztelését szakképzett és arra jogosult külső szervek is végezhetik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a biztonságos törléshez használt eszközöket és eljárásokat.
2. A szervezetnek meg kell határoznia, hogy milyen időközönként végzi vagy végezteti el a tesztelést.
3. Amennyiben a szervezet külső szolgáltatóval tervezi elvégeztetni a biztonságos törléshez alkalmazott eszközök és eljárások tesztelését, akkor a szervezetnek ki kell választania egy megfelelően képzett szolgáltatót ennek a tevékenységnek az elvégzésére. Emellett a szervezetnek valamilyen megállapodás keretében fel kell hatalmaznia a kiválasztott szolgáltatót a biztonságos törlésre és megsemmisítésre használt berendezések és eljárások tesztelésére.
4. A tesztelés során a szervezetnek gondoskodnia kell a biztonságos törléshez alkalmazott eszközökkel és eljárásokkal elvégzett tesztelés dokumentálásáról, mely tartalmazza a tesztelés eredményét és az esetlegesen felmerült problémák leírását.
5. A szervezetnek értékelnie kell a tesztelés eredményét, és ha szükséges, módosítania kell az eszközöket és eljárásokat a biztonságos törlés folyamatának javítása érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.8.6. Adathordozók törlése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MP-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

11.11. ADATHORDOZÓK TÖRLÉSE – RONCSOLÁSMENTES TECHNIKÁK

11.11. A szervezet roncsolásmentes adattörlési technikákat alkalmaz a meghatározott hordozható tárolóeszközökön, mielőtt azokat a szervezet által meghatározott körülmények között csatlakoztatná a rendszerhez.

MAGYARÁZAT

A hordozható tárolóeszközök kártékony kódot tartalmazhatnak, melyek általában az USB-porton vagy más bemeneten keresztül az EIR-be kerülhetnek és megfertőzhetik a szervezet EIR-jét. Az ilyen tároló eszközök ellenőrzése mindig ajánlott, viszont a törlés további biztosítékot nyújt arra nézve, hogy az eszközök mentesek a kártékony – akár még ismeretlen – kódoktól. A szervezet dönthet úgy, hogy roncsolásmentes adattörlési technikát alkalmaz a frissen vásárolt, vagy az ellenőrzésük alól kikerülő adathordozókon.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely hordozható tárolóeszközökön kíván roncsolásmentes adattörlési technikát alkalmazni. Ez azt jelenti, hogy az érintett szervezetnek törölnie kell minden adatot a hordozható tárolóeszközökről anélkül, hogy fizikailag károsítaná az eszközöket.
2. A szervezetnek meg kell határoznia, hogy milyen körülmények fennállása esetén csatlakoztat hordozható tárolóeszközt az EIR-hez.
3. A szervezetnek dokumentálnia kell a roncsolásmentes adattörlési folyamatot így biztosítva a nyomonkövethetőséget.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie/módosítania kell a roncsolásmentes adattörlési technikáit és eljárásait, így biztosítva, hogy a legújabb és legbiztonságosabb módszereket alkalmazza.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.8.6. Adathordozók törlése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MP-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a roncsolásmentes adattörlési technikákat igénylő hordozható tárolóeszközök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

11.12. ADATHORDOZÓK TÖRLÉSE – KETTŐS JÓVÁHAGYÁS

11.12. A szervezet kettős jóváhagyáshoz köti a meghatározott EIR adathordozóinak biztonságos törlését.

MAGYARÁZAT

Az érintett szervezet kettős jóváhagyáshoz köti az EIR-hez köthető adathordozó törlését, mely csak akkor történhet meg, ha két technikailag megfelelően képzett személy végzi a tevékenységet. Azok a személyek, akik az EIR-hez köthető adathordozók törlését végzik, rendelkeznek elegendő szakértelemmel ahhoz, hogy megállapítsák, a javasolt törlési technika/eljárás megfelel-e a jogszabályi követelményeknek, illetve az érintett szervezet belső szabályzatainak. A kettős jóváhagyás továbbá segít biztosítani, hogy a törlés a tervezett módon, illetve a valóságban is megtörténjen. A kettős jóváhagyást négy szem elvnek is nevezik. A csalás kockázatának csökkentése érdekében az érintett szervezet fontolóra veheti a kettős jóváhagyási feladatok több személy közötti rotációját.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek kettős jóváhagyáshoz kell kötnie az EIR-hez köthető adathordozó törlését, mely csak akkor történhet meg, ha két technikailag megfelelően képzett személy végzi a tevékenységet. Akik az EIR-hez köthető adathordozók törlését végzik, rendelkeznek elegendő szakértelemmel ahhoz, hogy megállapítsák, a javasolt törlési technika/eljárás megfelel-e a jogszabályi követelményeknek, illetve az érintett szervezet belső szabályzatainak.
2. A szervezetnek dokumentálnia kell a törlési folyamatot, beleértve a kettős jóváhagyást is, így biztosítva a megfelelő eljárás betartását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

11.2. Hozzáférés az adathordozókhoz

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

MP-6(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az adathordozók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

11.13. ADATHORDOZÓK TÖRLÉSE – ADATOK TÁVOLI TÖRLÉSE VAGY MEGSEMMISÍTÉSE

11.13. A szervezet kialakítja a képességet a távoli információtörlésre vagy felülírásra a meghatározott EIR-eken vagy rendszerelemeken, a szervezet által meghatározott feltételek teljesülése mellett.

MAGYARÁZAT

Az adatok távoli törlése vagy megsemmisítése védelemként szolgálhat az érintett szervezet EIR-jén és annak elemein található információk vonatkozásában, ha az EIR-en vagy annak elemein illetéktelen személyek átveszik az irányítást. A távoli információtörléssel vagy megsemmisítéssel összefüggő parancsok erős hitelesítést igényelnek, így segíthetnek csökkenteni annak a kockázatát, hogy illetéktelen személyek töröljék vagy megsemmisítsék az EIR-t, az ahhoz köthető elemet vagy eszközt. Az információtörlési vagy megsemmisítési funkciót számos módon lehet megvalósítani, beleértve az adatok többszöri felülírását vagy a titkosított adatok dekódolásához szükséges kulcs megsemmisítését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely EIR-ek vagy rendszerelemek esetében van szükség a távoli információtörlésre vagy megsemmisítésre.
2. A távoli információtörléssel vagy megsemmisítéssel összefüggő parancsok vonatkozásában a szervezetnek erős hitelesítést kell kialakítania, mely segíthet csökkenteni annak a kockázatát, hogy illetéktelen személyek töröljék vagy megsemmisítsék az EIR-t, azon tárolt adatokat, EIR-hez köthető elemet vagy eszközt.
3. A szervezetnek alkalmaznia kell az információtörlési vagy megsemmisítési funkciót. Ez többféleképpen megvalósítható, beleértve az adatok többszöri felülírását vagy a titkosított adatok dekódolásához szükséges kulcs megsemmisítését.
4. A szervezetnek meg kell határoznia, hogy milyen feltételek teljesülése esetén alkalmazza a távoli információtörlést vagy megsemmisítést.
5. A szervezetnek dokumentálnia kell a távoli információtörlést vagy megsemmisítést, hogy ki, mikor és milyen okból végezte el a törlést vagy megsemmisítést.

6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie/módosítania kell a távoli információtörlési vagy megsemmisítési képességét, így biztosítva annak hatékonyságát és naprakészségét.

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

MP-6(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek illetve a feltételek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

11.14. ADATHORDOZÓK HASZNÁLATA

11.14. A szervezet:

11.14.1. Korlátozza vagy tiltja a szervezet által meghatározott típusú adathordozók használatát a szervezet által meghatározott EIR-eken vagy rendszerelemeken, a szervezet által meghatározott irányítási mechanizmusok alkalmazásával.

11.14.2. Megtiltja a hordozható adattároló eszközök használatát a szervezeti EIR-ekben, ha azoknak nincs azonosítható tulajdonosa.

MAGYARÁZAT

Az EIR adathordozói lehetnek digitális és analóg adathordozók. Digitális adathordozók alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm. Ezen követelmény szabályait abban az esetben is alkalmazni kell, amennyiben valamilyen mobil eszköz rendelkezik adattárolási lehetőséggel p.: okostelefonok, tabletek, e-könyv olvasók. Ez a követelmény korlátozza bizonyos típusú adathordozók használatát az EIR-ekben, például korlátozza vagy tiltja a flash meghajtók vagy külső merevlemezek használatát. Az érintett szervezet korlátozhatja a hordozható tárolóeszközök használatát, például fizikailag elzárhatják a munkaállomásokat, ami azt jelenti, hogy megakadályozzák bizonyos külső portokhoz történő hozzáférést, illetve nem teszik lehetővé az említett eszközök csatlakoztatását, így azokat írni és olvasni sem lehet. A szervezetek korlátozhatják a hordozható tárolóeszközök használatát oly módon is, hogy csak a jóváhagyott, például a szervezet vagy más külső fél által biztosított eszközök csatlakoztathatóak, viszont a személyes tulajdonban álló eszközök kizárásra kerülnek. Végül a szervezetek korlátozhatják a hordozható tárolóeszközöket típustól függően. Az érintett szervezet tilthatja az írható, hordozható tárolóeszközök használatát, melyet akár logikai követelmény alkalmazásával ki lehet kényszeríteni. Az éirintett szervezet tulajdonosokat rendelhet a hordozható adattároló eszközökhöz csökkentve ezzel az eszközök használatával kapcsolatos kockázatot és egyúttal megteremti az eszközökkel kapcsolatos sérülékenységek kezelésének felelősségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell, illetve meg kell határoznia azokat a típusú adathordozókat, amelyek használatát korlátozni vagy tiltani kívánja az EIR-eken vagy rendszerelemeken, a szervezet által meghatározott irányítási mechanizmusok alkalmazásával.
2. A szervezetnek meg kell tiltania a hordozható adattároló eszközök használatát a szervezeti EIR-ekben, ha azoknak nincs azonosítható tulajdonosa.
3. A szervezet korlátozhatja a hordozható tárolóeszközök használatát.
4. A szervezet korlátozhatja a hordozható tárolóeszközök használatát oly módon is, hogy csak a jóváhagyott, például a szervezet vagy más, ellenőrzött külső fél által biztosított eszközök csatlakoztathatóak, viszont a személyes tulajdonban álló eszközök kizárásra kerülnek.
5. A szervezet korlátozhatja a hordozható tárolóeszközöket típustól függően.
6. A szervezetnek naplóznia, illetve rendszeresen ellenőriznie kell az adathordozók használatát, hogy biztosítsa a szabályok betartását és azonnal észlelje a szabályok megsértését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.113. Mobil eszközök hozzáférés-ellenőrzése

2.115. Külső elektronikus információs rendszerek használata

13.3.1. Viselkedési szabályok

1.13. Belső fenyegetés elleni program

17.98. Végrehajtható, de nem módosítható programok

17.116. Portok, illetve ki- és bemeneti eszközök hozzáférése

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

3.3.8.7. Adathordozók használata

ISO/IEC 27001:2023 REFERENCIA

A.5.10; A.7.10

NIST SP 800-53 REV.5 REFERENCIA

MP-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

11.15. ADATHORDOZÓK HASZNÁLATA – BIZTONSÁGOS TÖRLÉSNEK ELLENÁLLÓ ADATHORDOZÓK HASZNÁLATÁNAK TILTÁSA

11.15. A szervezet megtiltja a biztonságos törlésnek ellenálló adathordozók használatát a szervezeti EIR-ekben.

MAGYARÁZAT

A biztonságos törlésnek ellenálló adathordozók olyan eszközök, melyek ellenállnak a roncsolásmentes törlési eljárásoknak vagy amelyeknél a biztonságos törlés nem szabványos módon támogatott. Az ilyen típusú adathordozók közé tartozhatnak például az SSD-k és a hordozható USB adattárolók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie az EIR-ekben jelenleg használt adathordozókat annak érdekében, hogy megállapítsa, melyek azok, amelyek ellenállnak a biztonságos törlésnek.
2. A szervezetnek megtiltja a biztonságos törlésnek ellenálló adathordozók használatát a szervezeti EIR-ekben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

11.8. Adathordozók törlése

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

MP-7(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

11.16. ADATHORDOZÓK VISSZAMINŐSÍTÉSE

11.16. A szervezet:

11.16.1. Létrehoz egy, a szervezet által meghatározott adathordozó-visszaminősítési folyamatot, amely magában foglalja a törlendő információ biztonsági besorolásának megfelelő szintű mechanizmusok alkalmazását.

11.16.2. Ellenőrzi, hogy az adathordozó-visszaminősítési folyamat megfelel-e az eltávolítandó információ biztonsági besorolásának, valamint az információt potenciálisan átvevők hozzáférési jogosultságainak.

11.16.3. Azonosítja a visszaminősítést igénylő adathordozókat.

11.16.4. Meghatározott folyamat segítségével visszaminősíti az azonosított adathordozókat.

MAGYARÁZAT

Az adathordozó-visszaminősítési folyamat alkalmazható olyan digitális és analóg adathordozókra melyek hamarosan leselejtezésre kerülnek és ezáltal elhagyják a szervezet területét. Az alkalmazás független attól, hogy az adathordozót hordozhatónak tekinti-e az érintett szervezet vagy sem. Az EIR-hez köthető adathordozóról a visszaminősítési folyamat során az érintett szervezet eltávolítja az információt az adathordozóról, tipikusan biztonsági kategória vagy besorolási szint alapján, úgy, hogy az információt ne lehessen visszanyerni vagy újraalkotni. Adathordozó-visszaminősítésről beszélünk akkor is, ha magában foglalja bizonyos információk törlését, ezzel lehetővé téve a szélesebb körű megismerést és terjesztést. A visszaminősítés biztosítja, hogy az adathordozó üres területe ne tartalmazzon információt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet létre kell hoznia egy adathordozó-visszaminősítési folyamatot, amelyet a szervezet maga határoz meg. Ez a folyamat magában foglalja a törlendő információ biztonsági besorolásának megfelelő szintű mechanizmusok alkalmazását.
2. A szervezetnek ellenőriznie kell, hogy az adathordozó-visszaminősítési folyamat megfelel-e az eltávolítandó információ biztonsági besorolásának, valamint az információt potenciálisan átvevők hozzáférési jogosultságainak.
3. A szervezet azonosítania kell a visszaminősítést igénylő adathordozókat.

4. A szervezetnek a meghatározott folyamat segítségével vissza kell minősítenie az azonosított adathordozókat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie (módosítania) kell az adathordozó-visszaminősítési folyamatot így biztosítva annak hatékonyságát és naprakészségét.

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

MP-8

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

11.17. ADATHORDOZÓK VISSZAMINŐSÍTÉSE – FOLYAMAT DOKUMENTÁCIÓJA

11.17. A szervezet a szervezet által meghatározott gyakorisággal teszteli a visszaminősítés során használatos eszközöket és eljárásokat, hogy biztosítsa a visszaminősítési műveletek sikeres végrehajtását.

MAGYARÁZAT

Az érintett szervezet dokumentálja a visszaminősítési folyamatot az alábbi információk megadásával: a használt visszaminősítési technika, a visszaminősített adathordozó azonosítószáma, illetve a személy megnevezése, aki a visszaminősítési műveletet engedélyezte és/vagy végrehajtotta.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

-

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

MP-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

11.18. ADATHORDOZÓK VISSZAMINŐSÍTÉSE – BERENDEZÉS TESZTELÉSE

11.18. A szervezet a szervezet által meghatározott gyakorisággal teszteli a visszaminősítés során használatos eszközöket és eljárásokat, hogy biztosítsa a visszaminősítési műveletek sikeres végrehajtását.

MAGYARÁZAT

-

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania és be kell szereznie az adathordozók visszaminősítésére használt eszközöket.
2. A szervezetnek meg kell határoznia a visszaminősítési eszközök és eljárások tesztelésének gyakoriságát.
3. A szervezetnek rendszeresen tesztelnie kell a visszaminősítés során használt eszközöket és eljárásokat.
4. A szervezetnek dokumentálnia kell a visszaminősítési teszt eredményeit. Ez magában foglalja az esetleges hibák, problémák dokumentálását, valamint az elvégzett visszaminősítési műveletek rögzítését.
5. A szervezetnek rendszeresen értékelnie kell a visszaminősítési tesztek eredményeit. Ha a tesztek során problémák merülnek fel, az érintett szervezetnek meg kell találnia a megoldást, és szükség esetén módosítania kell a visszaminősítési eszközöket és eljárásokat.

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

MP-8(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024