

BIZTONSÁGOS TÖRLÉSI MEGOLDÁSOK

VFP3 KiberVéd - NIS2 Audit felkészítés szakmai
iránymutatás 2026/14

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.28	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1. VEZETŐI ÖSSZEFOGLALÓ

Jelen iránymutatás a szervezeti adathordozók és adattárolási környezetek biztonságos törlésének gyakorlati követelményeit foglalja össze. A jogi alapot a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) és a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet) adja. A technológiai és eljárási ajánlások a NIST SP 800-88 Revision 2 2025 szeptemberében kiadott végleges változatának szemléletét követik.

A legfontosabb következtetések:

- A fájl törlése, a partíció eltávolítása, a gyorsformázás vagy a gyári alaphelyzetbe állítás önmagában nem minden esetben jelent biztonságos törlést.
- A törlési módszert nem a használt operációs rendszer, hanem az adathordozó fizikai technológiája, a kezelt információ biztonsági besorolása, az eszköz állapota és a tervezett további felhasználás alapján kell kiválasztani.
- Újrahasznosítandó SSD/NVMe eszköz esetén elsődlegesen a szabványos, eszközszintű „sanitize” vagy megfelelően igazolt kriptográfiai törlés alkalmazandó; a többmenetes felülírás SSD-n nem korszerű és nem megbízható megoldás.
- A szervezetnek a teljes adattárolási láncot kezelnie kell, fizikai meghajtók, RAID-tömbök, virtuális lemezek, pillanatképek, replikák, biztonsági mentések, felhős verziók és törlési késleltetések egyaránt a hatókör részei lehetnek.
- A megfelelés nem csak a törlési műveletből áll. Szükséges az előzetes megőrzési ellenőrzés, a módszerválasztás dokumentálása, a művelet eredményének ellenőrzése és validálása, valamint az eszközazonosítóhoz kötött auditbizonyíték.
- A törlés megkezdése előtt minden esetben ellenőrizni kell a jogszabályi, szerződéses, peres vagy hatósági megőrzési kötelezettségeket. A biztonságos törlési eljárás nem írhatja felül a kötelező irat- vagy adatmegőrzést; a törlés csak jóváhagyott megőrzési idő lejárta után hajtható végre.

2. A VIZSGÁLANDÓ KÉRDÉS

Az adathordozók életciklusának végén a szervezetnek olyan eljárást kell működtetnie, amely megakadályozza, hogy a leselejtezett, értékesített, visszaadott, garanciális javításra átadott vagy más célra újra felhasznált eszközről jogosulatlan személyek adatot állítsanak helyre.

Az iránymutatás arra keresi a választ, hogy mikor elegendő a logikai törlés vagy felülírás, mikor szükséges eszközszintű törlés, kriptográfiai törlés vagy fizikai megsemmisítés. Vizsgálja továbbá, hogy mely konkrét parancsok, protokollok és eszköztípusok alkalmazhatók HDD,

SSD/NVMe, mobil, felhő és mentési környezetben. Segítséget nyújt abban is, hogy hogyan kell adminisztrálni a törlést.

A biztonságos törlési eljárások megértéséhez fontos megkülönböztetni a logikai és a fizikai törlési technikákat. Logikai törlési technika szoftver vagy más eszköz segítségével, az adathordozó interfészén (pl. gazdagép-illesztőn) keresztül történő, rendszeres adatfelülírás vagy -eltávolítás. A logikai technikák célja, hogy az adathordozó használható állapotban maradjon. Fizikai törlési technikák külső fizikai beavatkozással végrehajtott adatmegsemmisítés. A fizikai technikák jellemzően az adathordozó használhatatlanná válásával járnak. Kivételt képez a demagnetizálás, amely bizonyos mágneses adathordozókon a hordozó megőrzése mellett is végrehajtható.

3. ALKALMAZANDÓ KÖVETELMÉNYEK

A Kiberbiztonsági tv. 5. §-a rögzíti, hogy az elektronikus információs rendszerek (a továbbiakban: EIR) védelmét azok teljes életciklusában, a kockázatokkal arányosan kell biztosítani. A védelemnek az adatok mellett az EIR elemekre, az alkalmazott eszközökre, eljárásokra és az ezeket kezelő személyekre is ki kell terjednie.

„5. §(1) Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok, információk és az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása

vonatkozásában a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet.

(2) Az elektronikus információs rendszer védelme keretében az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezet, az adatkezelő vagy az adatfeldolgozó által, adott cél érdekében

a) az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat

b) az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint

c) az a) és b) pontban foglaltakat kezelő személyek együttesének védelmét is biztosítani szükséges.”

[2024. évi LXIX. törvény 5. § (1)–(2) bekezdés]

Egyrészt a törlésnek a leselejtezés, az ellenőrzési körből kikerülés vagy az újrahasználat előtt meg kell történnie. Másrészt a módszerválasztásnak kockázatarányosnak kell lennie. Ebből

következik, hogy egyetlen, minden eszközre azonos „törlőprogram” alkalmazása nem tekinthető kellően megalapozott megoldásnak.

„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.”

[7/2024. (VI. 24.) MK rendelet 2. melléklet 11.8. követelménycsoport]

(„Alap” biztonsági osztály)

A követelmény teljesítése érdekében a szervezetnek olyan nyomon követhető eljárást célszerű kialakítania, amely legalább az adathordozó azonosítását, a törlési módszer előzetes jóváhagyását, a végrehajtás dokumentálását, az eredmény ellenőrzését, valamint a sikertelen vagy nem egyértelmű műveletek kezelését tartalmazza. A törlési jegyzőkönyv, az eszköz által előállított napló és a megsemmisítési igazolás ennek auditbizonyítékaul szolgálhat.

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

[7/2024. (VI. 24.) MK rendelet 2. melléklet 11.10. követelménycsoport]

(„Magas” biztonsági osztály)

A tesztelésnek célszerű kiterjednie a törlőszoftverek és parancssori eszközök támogatott verzióira, a sanitize parancsok tényleges működésére, a törlési naplók előállítására, a degausser (mágneses adatmentesítő) vagy megsemmisítő berendezés megfelelő működésére, valamint a sikertelen műveletek észlelésére. A tesztelés gyakoriságát kockázatalapon kell meghatározni, továbbá indokolt soron kívüli tesztet végrehajtani olyan jelentős változásokat követően, amelyek az adatmentesítési folyamat megbízhatóságát befolyásolhatják, így különösen jelentős szoftver- vagy verzióváltás, firmware-frissítés, új adathordozó-technológia bevezetése, illetve az adatmentesítéshez alkalmazott eszköz vagy berendezés cseréje esetén.

4. JAVASOLT MÓDSZERTAN

A NIST szabvány a biztonságos törlést olyan folyamatként határozza meg, amely a céladat elérését egy meghatározott erőfeszítési szint mellett megvalósíthatatlanná teszi. A módszert az adat bizalmassága, a várható helyreállítási képesség, az adathordozó jövőbeli sorsa és a szervezeti kontroll alapján kell kiválasztani. A megfelelő eljárás kiválasztását minden esetben egy dokumentált, kockázatalapú döntési folyamatnak kell megelőznie, figyelembe véve az adatok bizalmassági besorolását és az adatmentesítés lehetséges kockázatait. Az alábbiakban áttekintjük az alkalmazott eljárás típusokat.

4.1 Tisztítás (Clear)

A „Clear” kategória logikai (szoftveres) törlési eljárásokat takar, amelyek célja az adatok eltávolítása az adathordozó összes felhasználó által hozzáférhető tárterületéről. A Clear logikai törlési módszer a felhasználó által elérhető tárolóterületeket tisztítja meg, így az adatok egyszerű, nem invazív módszerekkel nem állíthatók helyre. Tipikus megoldás a teljes címezhető terület felülírása vagy dokumentált gyártói visszaállítás. A hordozó általában újra használható marad.

Olyan adathordozók esetében alkalmazható, amelyeket a szervezeten belül újra felhasználnak, és nem tartalmaztak kiemelten érzékeny vagy magas biztonsági besorolású adatokat. Papíralapú adathordozón nem alkalmazható. Flashalapú tárolón a felülírás csak az elérhető területekre terjed ki, ezért magasabb kockázat esetén önmagában nem elegendő.

4.2 Mélytisztítás (Purge)

A „Purge” kategória jóval magasabb szintű biztonságot garantál. Célja, hogy az adatokat úgy távolítsa el vagy tegye olvashatatlaná, hogy azok a legkorszerűbb laboratóriumi, hardveres adat-helyreállítási technikákkal se legyenek visszaállíthatók. Az adathordozó potenciálisan újrahasználható marad.

A Purge kategóriába tartozó leggyakoribb technikai megoldások:

- Kriptográfiai törlés, azaz hardveres titkosítással rendelkező eszközök esetén a titkosítási kulcs megsemmisítése, ami azonnal olvashatatlaná teszi a tárolt adatokat.
- Blokk szintű törlés, flash alapú memóriák (pl. SSD-k, okostelefonok) beépített, gyártó által biztosított biztonsági törlési parancsainak futtatása.
- Lemágnesezés (Degaussing), erős mágneses mező alkalmazása a mágneses elven működő adathordozók (pl. hagyományos HDD-k, mágnesszalagok) esetén. A lemágnesezés megbontja a mágneses mintázatot, ezáltal visszavonhatatlanul törli az adatokat. Az eljárás többnyire fizikai károsodást okoz a mágneslemezek vezérlőmechanizmusában, így az adathordozó a művelet után többé nem lesz használható, ezért hatása a megsemmisítéssel egyenértékű.

A NIST ajánlása szerint a Purge módszert célszerű alkalmazni, ha a Clear által nyújtott védelem az adott információbiztonsági kockázat mellett nem biztosít megfelelő védelmet, de a hordozó megsemmisítése nem indokolt. A módszert kockázatalapon kell kiválasztani és az eredmény megfelelőségét külön validálni szükséges.

4.3 Megsemmisítés (Destroy)

A Destroy fizikai megsemmisítési módszer, amely az adat helyreállítását korszerű laboratóriumi eljárásokkal is ellehetetleníti, és az adathordozót további használatra alkalmatlanná teszi. Különösen hibás, elavult, ismeretlen képességű vagy megbízhatóan nem törölhető eszközöknél indokolt.

Az egyszerű fűrés, hajlítás vagy részleges roncsolás önmagában nem feltétlenül elegendő. A megsemmisítés módját és a szükséges maradványméretet az adathordozó típusához,

adatsűrűségéhez és a biztonsági követelményekhez kell igazítani. Lehetséges technológiák a darálás (shredding), zúzás, elégetés (incineration), savas roncsolás, vagy olvasztás.

A módszerválasztást dokumentált és kockázatalapú döntési folyamatban kell elvégezni. Az egyetlen, minden eszközre alkalmazott azonos törlési eljárás használata nem tekinthető kellően megalapozott megoldásnak. A megfelelő módszer (Clear, Purge vagy Destroy) meghatározásához a NIST SP 800-88 szabvány döntési folyamatát javasolt követni.

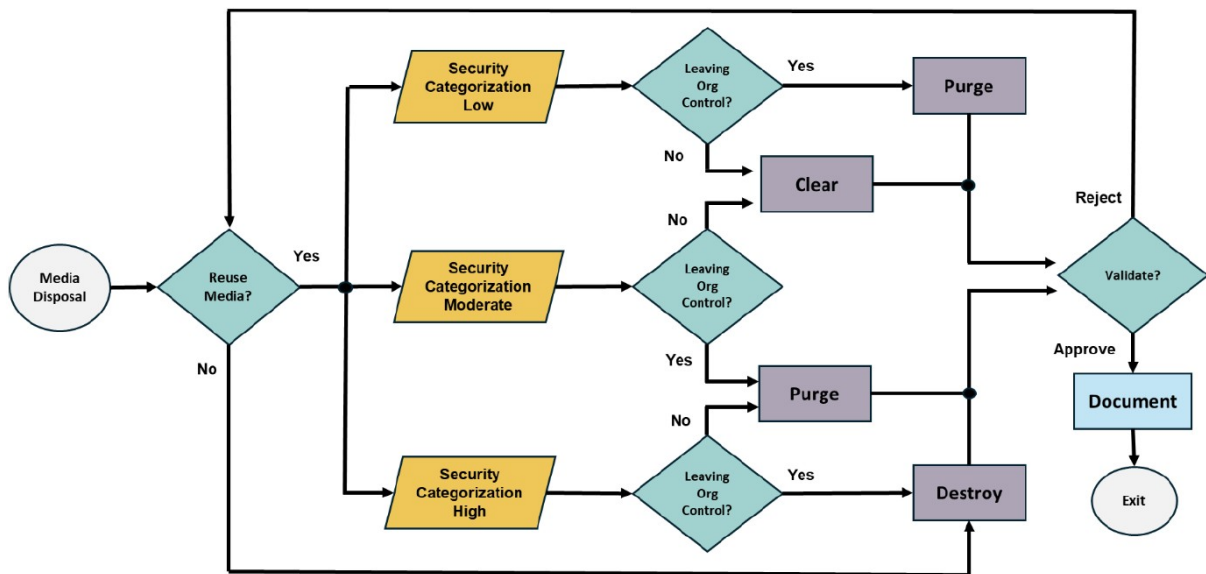


Fig. 1. Sanitization and disposition decision flow

1. ábra A törlési módszer kiválasztásának döntési folyamata az NIST SP 800-88r2 alapján¹

4.4 A törlési folyamat

Az alábbiakban ismertetjük a törlési folyamat lépéseit.

1. Első lépés az adatok törölhetőségének jogi és adminisztratív ellenőrzése. Ellenőrizni kell, hogy az adathordozó és a rajta lévő adat egyáltalán törölhető-e. Kötelező megőrzés, jogi vagy hatósági zárolás, folyamatban lévő incidensvizsgálat vagy bizonyítékmegőrzés esetén a törlést fel kell függeszteni.
2. Ezt követi az adathordozó további sorsának meghatározása (újrahasználat). El kell dönteni, hogy az adathordozót a jövőben újra fel kívánják-e használni, akár a szervezeten belül, akár azon kívül.
 - a) Nem használják újra, ha az adathordozó hibás, elavult, vagy a szervezet döntése alapján biztosan nem kerül már használatba, a választandó eljárás a megsemmisítés (Destroy).
 - b) Ha az eszközt (vagy alkatrészeit) újra használni fogják, a folyamat a 3. lépéssel folytatódik.

¹ NIST Special Publication 800 NIST SP 800-88r2 Guidelines for Media Sanitization

3. Eszköz-, adat- és hatókör-azonosítás, rögzíteni kell az adathordozó alapvető azonosító adatait, típusát és titkosítási állapotát, továbbá a rajta kezelt adatok legmagasabb biztonsági besorolását. A törlés hatókörét ki kell terjeszteni minden kapcsolódó adatpéldányra és tárolási helyre, így különösen a snapshotokra, replikákra, mentésekre, gyorsítótárakra, tartalék vagy hibás meghajtókra, kulcspéldányokra és szolgáltatói másolatokra.
4. A felügyeleti kör vizsgálata és a törlési módszer kiválasztásának alapja az adatok biztonsági besorolása és az adathordozó jövőbeli fizikai helyzete (elhagyja-e a szervezet közvetlen felügyeleti körét) alapján kell kijelölni a végleges törlési kategóriát:
 - Alacsony vagy közepes biztonsági besorolású adatok esetén:
 - Ha az adathordozó a szervezeten belül marad (pl. másik osztály/munkatárs kapja meg), akkor Tisztítás (Clear) eljárás alkalmazandó.
 - Ha az adathordozó elhagyja a szervezetet (pl. adományozás, eladás, lízingcégnek történő visszaadás), akkor Mélytisztítás (Purge) eljárás kötelező.
 - Magas biztonsági besorolású adatok esetén:
 - Ha az adathordozó a szervezeten belül marad, akkor Mélytisztítás (Purge) eljárás alkalmazandó.
 - Ha az adathordozó elhagyja a szervezetet, akkor Megsemmisítés (Destroy) eljárás kötelező.
5. Ellenőrzésként rögzíteni kell a befejezési státuszt, a hibákat, anomáliákat, az eszköz állapotát és destruktív eljárásnál a keletkezett maradvány jellemzőit. A validálás és lezárás során a kijelölt felelős dönt az eredmény elfogadásáról. Elutasítás esetén másik technikát, ismételt végrehajtást vagy magasabb biztonságú módszert kell alkalmazni.
6. Dokumentálás, a kiválasztott és végrehajtott törlési vagy megsemmisítési eljárást, a használt technológiát és a végeredményt hitelt érdemlően jegyzőkönyvezni kell. A folyamat a törlés sikerességének visszaellenőrzésével és a jegyzőkönyv jóváhagyásával zárul. Ezt követően frissíteni kell az eszköznyilvántartást és az átadási vagy megsemmisítési dokumentumokat. A törlés dokumentálására a jegykezelő rendszert a legcélszerűbb eszköz, de természetesen más megoldás is elfogadható.

5. A TÖRLÉSI EREDMÉNY ELLENŐRZÉSE

A kiválasztott eljárástól és tárolási technológiától függetlenül ellenőrizni kell, hogy a törlési művelet sikeresen befejeződött-e. Ennek keretében vizsgálni kell az alkalmazott eszköz vagy parancs befejezési állapotát, a naplózott hibákat, a kihagyott adatterületeket és az esetleges rendellenességeket.

„11.9. A szervezet felülvizsgálja, jóváhagyja, nyomon követi, dokumentálja és ellenőrzi az adathordozók biztonságos törlésével és megsemmisítésével kapcsolatos tevékenységeket.”

[7/2024. (VI. 24.) MK rendelet 2. melléklet 11.9. követelménycsoport]
(„Magas” biztonsági osztály)

Sikertelen, megszakadt vagy nem egyértelmű eredmény esetén a törlési folyamatot meg kell ismételni, másik igazolt módszert kell választani, vagy fizikai megsemmisítést kell alkalmazni. A végrehajtást és annak eredményét olyan módon kell dokumentálni, hogy az eszköz, az alkalmazott eljárás, a végrehajtó személy, az időpont és az ellenőrzés eredménye utólag is azonosítható legyen.

6. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- NIST Special Publication 800-88 Revision 2, Guidelines for Media Sanitization, Final

MELLÉKLET I. KONKRÉT TÖRLÉSI TECHNOLÓGIÁK ADATHORDOZÓ TÍPUSONKÉNT

I.1. Az eljárások alkalmazásának feltételei és a felelősség kizárása

Az e mellékletben ismertetett törlési, felülírási, kriptográfiai törlési és fizikai megsemmisítési eljárásokat kizárólag olyan személy végezheti, aki az érintett adathordozó-típus, tárolási technológia és törlési módszer szakszerű alkalmazásához szükséges szakértelemmel, gyakorlattal és technikai feltételekkel rendelkezik. Az eljárások szakszerűtlen végrehajtása a törlés eredménytelenségét, az adatok nem szándékolt és helyreállíthatatlan elvesztését, illetve az adathordozó vagy az informatikai eszköz károsodását idézheti elő.

A Szabályozott Tevékenységek Felügyeleti Hatósága nem vállal felelősséget az iránymutatásban ismertetett eljárások alkalmazásáért és azok eredményességéért. Nem vállal felelősséget továbbá az eljárások alkalmazásából eredő esetleges károkért, illetve egyéb jogi vagy ténybeli következményekért sem. Az adott eljárás kiválasztása, szakszerű végrehajtása, valamint az eredmény ellenőrzése és validálása az eljárást alkalmazó szervezet felelősségi körébe tartozik.

I.2. Gyakorlati törlési eljárások

Az alábbi alfejezetek a jelenleg elterjedt tárolási technológiákhoz alkalmazandó, gyakorlatban végrehajtható eljárásokat foglalják össze. A konkrét törlési eljárás kiválasztása előtt minden esetben ellenőrizni kell a gyártói dokumentációt, az alkalmazandó technikai szabványt és az adott firmware által ténylegesen támogatott funkciókat.

I.2.1. HDD-meghajtók

Szervezetén belüli, alacsonyabb kockázatú újrahasználát esetén a teljes, felhasználó által címezhető tárolóterület egyszeri, blokkszintű felülírása Clear technikaként alkalmazható. A műveletnek a teljes meghajtóra kell kiterjednie; a fájl-, partíció- vagy fájlrendszer szintű törlés önmagában nem elegendő. Korszerű HDD-knél a többmenetes felülírás általában nem biztosít arányos többletvédelmet.

Purge szinthez elsődlegesen a meghajtó által támogatott, szabványosított eszköz szintű sanitize funkció alkalmazandó. ATA-környezetben ilyen lehet az ATA SANITIZE DEVICE Overwrite, öntitkosító meghajtón a Crypto Scramble vagy más igazolt kriptográfiai törlés, régebbi eszközön pedig az ATA SECURITY ERASE UNIT vagy Enhanced Erase.

A parancs elnevezése önmagában nem igazolja a Purge szintet. Ellenőrizni kell az adott meghajtómodell és firmware esetében a művelet hatókörét, a tartalék vagy áthelyezett területek kezelését, valamint a sikeres befejezés és a hibák visszajelzését.

A végrehajtást a meghajtó állapotjelzései, a törlőeszköz naplója és a hibakódok alapján ellenőrizni kell, majd külön validálni szükséges, hogy az eredmény a kezelt adatok bizalmassága és az eszköz további felhasználása alapján elfogadható-e. Sikertelen vagy nem igazolható törlés esetén fizikai megsemmisítésre kell áttérni.

Megfelelően méretezett és igazolt degausser mágneses HDD-n Purge technikaként alkalmazható, de önmagában nem minősül Destroy módszernek. Destroy esetén a mágneses tányérokat olyan,

az adathordozó típusához igazított és validált fizikai eljárással kell helyreállíthatatlanná tenni, amely megfelel az alkalmazott technikai szabványnak és az adatok bizalmassági szintjének. Alkalmazható például megfelelő dezintegrálás, olvasztás vagy ellenőrzött ipari égetés. Aprítás vagy darálás csak akkor fogadható el, ha az elért maradványméret és a módszer alkalmassága igazolt.

A meghajtó burkolatának vagy elektronikájának roncsolása, illetve az egyszerű fúrás, hajlítás vagy részleges darabolás nem elegendő. A degaussingot külön Destroy eljárás követheti, ha azt az adatok bizalmassága, a szervezet belső szabályzata vagy a maradványkockázat indokolja.

1.2.2. NVMe-és SSD-meghajtók

Az SSD-meghajtóknál (amelyek jellemzően NVMe vagy SATA protokollt használnak) elsődlegesen dedikált, eszközszintű sanitize funkciót kell alkalmazni. A gazdarendszerből végzett felülírás csak a logikailag címezhető területekre terjed ki, és nem feltétlenül éri el a túlbővítési területet, a tartalék cellákat, az áthelyezett blokkokat vagy más, kizárólag a vezérlő által kezelt tárolóhelyeket.

NVMe-környezetben konkrét implementációs megoldás az NVMe sanitize parancs, amely a meghajtó képességeitől függően az alábbi műveleteket támogathatja:

- Block Erase, a NAND memóriablokkok alacsony szintű törlése;
- Crypto Erase, a felhasználói adatok visszafejtéséhez szükséges médiakulcs törlése vagy megváltoztatása;
- Overwrite, az érintett tárolóterületek meghatározott mintával történő felülírása.

A hagyományos sanitize művelet az NVM-alrendszer felhasználói adataira, így a nem felejtő médiára, gyorsítótárakra, metaadatokra, nem kiosztott és túlbővítési területekre is kiterjedhet.

A művelet támogatását a vezérlő képességadatai, eredményét pedig a Sanitize Status Log alapján kell ellenőrizni. Linux-környezetben implementációs példaként az `nvme id-ctrl`, az `nvme sanitize` és az `nvme sanitize-log`, újabb támogatott környezetben pedig az `nvme sanitize-ns` funkció használható. A paramétereket minden esetben az adott eszköz képességei és a gyártói dokumentáció alapján kell meghatározni.

Az NVMe Format NVM Secure Erase vagy Crypto Erase opciója dokumentált esetben alternatív technika lehet, de nem tekinthető automatikusan a sanitize teljes értékű helyettesítőjének. Hatóköre névtérhez kötött lehet, és nem biztosítja minden esetben a sanitize művelethez kapcsolódó állapotkövetési és megszakításkezelési képességeket.

SATA SSD-n alkalmazható az eszköz által támogatott ATA SANITIZE DEVICE, illetve igazolt öntitkosító meghajtón kriptográfiai törlés. TCG Opal eszköznél a Revert, RevertSP vagy PSID használata csak akkor fogadható el, ha igazolt, hogy a művelet ténylegesen eltávolítja a felhasználói adatokat és megsemmisíti a releváns médiakulcsokat. Figyelembe kell venni az eszköz életciklus-állapotát, a `KeepGlobalRangeKey` beállítást és azt is, hogy egy megszakadt művelet eredménye bizonytalan lehet.

Ha a meghajtó nem támogat megfelelő sanitize funkciót, a művelet sikertelen, vagy a vezérlő nem működik, magasabb bizalmasságú adatok esetén validált fizikai megsemmisítést kell alkalmazni. Ennek valamennyi NAND memóriakomponensre ki kell terjednie; a burkolat, a nyomtatott áramköri lap vagy kizárólag a vezérlőchip roncsolása nem elegendő. A megsemmisítési módszert az adathordozó felépítéséhez és az alkalmazandó technikai szabványhoz kell igazítani.

1.2.3. USB-meghajtók, SD- és microSD-kártyák

Alacsonyabb kockázatú, szervezeten belüli újrahasználát esetén a teljes, felhasználó által címezhető kapacitás blokkszintű felülírása Clear technikaként alkalmazható. A műveletnek a teljes logikai eszközre ki kell terjednie, és naplózni kell legalább az eszköz azonosítóját, kapacitását, a feldolgozott területet, az eredményt és az esetleges írási hibákat. A fájl törlés, partíció törlés és gyorsformázás önmagában nem elegendő.

A flashalapú adathordozók vezérlője tartalék, hibás vagy áthelyezett cellákat is kezelhet, amelyek a gazdarendszerről nem címezhetők. Emiatt a teljes logikai kapacitás sikeres felülírása Clear eredményt igazolhat, de önmagában nem tekinthető Purge technikának. SD-kártyánál azt is ellenőrizni kell, hogy az alkalmazott eszköz kezeli-e az esetleges védett tárolóterületet.

Purge technikaként csak olyan gyártói, eszközszintű sanitize vagy kriptográfiai törlési funkció fogadható el, amelynek hatóköre, működése és sikeres végrehajtása dokumentált. Hardveresen titkosított USB-meghajtón a kriptográfiai törlés akkor megfelelő, ha az adatok kezdetől megfelelő titkosítással védettek, a médiakulcs egyedi, és annak valamennyi helyreállítási vagy másolati példányáig igazolhatóan megsemmisül.

Ha megfelelő Purge funkció nem áll rendelkezésre, és a Clear után fennmaradó kockázat az adatok bizalmassága vagy az eszköz külső átadása miatt nem elfogadható, validált fizikai megsemmisítést kell alkalmazni. A megsemmisítésnek valamennyi flashmemória-komponensre ki kell terjednie; a burkolat, az USB-csatlakozó vagy kizárólag a vezérlőchip roncsolása nem elegendő. A végrehajtott módszer megfelelőségét minden esetben ellenőrizni és validálni kell.

1.2.4. Mobileszközök

Szervezeti tulajdonú, korszerűen titkosított mobileszközön MDM- vagy UEM-rendszerről kezdeményezett teljes eszköztörlést, illetve a gyártó által dokumentált teljes tartalom- és beállítástörlési funkciót kell alkalmazni.

Apple-eszközökön erre szolgál az Erase All Content and Settings, MDM-környezetben pedig az EraseDevice parancs. Támogatott eszközön a művelet törli az effaceable storage-ban tárolt kulcsokat, ezáltal a felhasználói adatokat kriptográfiailag hozzáférhetetlenné teszi. A pontos támogatást és előfeltételeket az adott eszközmodell és operációsrendszer-verzió alapján kell ellenőrizni.

Android Enterprise környezetben a WIPE parancs vállalati tulajdonú eszközön gyári visszaállítást, személyes tulajdonú, munkaprofilos eszközön pedig a munkaprofil törlését kezdeményezi. A művelet paraméterezésével kezelhető lehet a külső tárhely, az eSIM és a Factory Reset Protection is.

A törlés során vagy azt követően külön kezelni kell:

- az eSIM-profil és a fizikai SIM-kártyát;
- a cserélhető memóriakártyát;
- a felhőben tárolt eszközmentéseket;
- az aktiválási vagy Factory Reset Protection zárolást;
- a gyártói és vállalati fiók-hozzárendeléseket;
- az MDM/UEM-regisztrációt;
- a szerveroldali tanúsítványokat, tokeneket és aktív munkameneteket.

A teljes eszköztörlés csak akkor minősíthető Purge eredményű kriptográfiai törlésnek, ha a titkosítás megfelelő működése, a releváns kulcsok érvénytelenítése, a művelet hatóköre és sikeres végrehajtása igazolt. Ennek hiányában a gyári visszaállítást Clear technikaként kell kezelni. Ez különösen Android-eszközöknél fontos, ahol a konkrét eredményt a gyártói dokumentáció és az eszköz tényleges megvalósítása alapján kell értékelni.

1.2.5. Szerverek, RAID-rendszerek, tárolótömbök és tartós memória

Szervereknél és központi tárolórendszereknél a törlés hatókörét valamennyi olyan fizikai és logikai komponensre ki kell terjeszteni, amelyen a céladat, annak másolata vagy a helyreállítását lehetővé tevő metaadat előfordulhat. A logikai kötet vagy RAID-konfiguráció törlése önmagában nem biztosít megfelelő adathordozó-szintű törlést.

A hatókörbe szükség szerint be kell vonni:

- az aktív HDD-, SSD-, SAS-, SATA- és NVMe-meghajtókat;
- a hot spare és global spare meghajtókat;
- a cache-meghajtókat és a nem felejtő vagy akkumulátorral védett vezérlőcache-t;
- a vezérlőkártyák tartós memóriáját;
- az NVRAM-, NVDIMM- és más persistent memory modulokat;
- a redundáns vezérlőmodulokat;
- a korábban kivett hibás meghajtókat;
- a konfigurációs, napló- és metaadat-területeket.

A gyártói array-szintű secure erase, sanitize vagy kriptográfiai törlés csak akkor fogadható el, ha dokumentáltan megállapítható, hogy mely fizikai adathordozókra és tartós komponensekre terjed ki, milyen technikát hajt végre, hogyan kezeli a spare és hibás meghajtókat, valamint milyen befejezési és hibaállapotot biztosít. A közös titkosítási kulcs törlése kizárólag akkor alkalmazható, ha a kulcs hatóköre, valamennyi példánya és az érintett adathordozók köre egyértelműen igazolható.

Ha a tárolótömb lehetővé teszi az ATA, SCSI vagy NVMe sanitize parancsok fizikai meghajtókhoz történő továbbítását, minden meghajtó eredményét külön ellenőrizni kell. Ha a parancstovábbítás vagy a hatókör nem igazolható, a meghajtókat közvetlenül, megfelelő interfészen kell kezelni, vagy fizikai megsemmisítésre kell áttérni.

Tartós memória és támogatott NVDIMM esetén a gyártó által meghatározott secure erase, crypto erase vagy teljes overwrite eljárást kell alkalmazni. Linux-környezetben implementációs példa lehet az `ndctl sanitize-dimm --crypto-erase` vagy `--overwrite`; aszinkron felülírásnál a művelet tényleges befejezését külön is ellenőrizni kell. Az újraindítás, áramtalanítás vagy fájlrendszer-törlés nem elegendő nem felejtő memória esetén.

A törlési folyamat csak akkor zárható le, ha valamennyi érintett komponens sikeres eredménye igazolt. A nem elérhető, hibás vagy nem megbízhatóan törölhető adathordozót validált fizikai megsemmisítéssel kell kezelni.

1.2.6. Virtuális gépek, virtuális lemezek és konténeres környezetek

Virtuális környezetben a törlés hatókörét a céladat valamennyi előfordulására ki kell terjeszteni. Ide tartozhatnak különösen:

- a virtuális lemezek;
- snapshotok és checkpointok;
- exportok;
- memória-, suspend-, hibernációs és swap állományok;
- ideiglenes lemezek;
- konténerek írható rétegei és ideiglenes kötetei;
- releváns image layerek, registrypéldányok és build cache-ek;
- replikák, archivált példányok és biztonsági mentések.

A virtuális gép, konténer vagy namespace törlése elsősorban a platformon nyilvántartott logikai objektumokat távolítja el. Ez önmagában nem igazolja a snapshotok, külső mentések, node-on tárolt példányok, registry rétegek vagy a mögöttes fizikai tároló blokkjainak biztonságos törlését. A Kubernetes szemétygyűjtése az ismert függő objektumokat és használaton kívüli image-eket kezelheti, de nem terjed ki automatikusan minden külső vagy szolgáltatói adatpéldányra.

PersistentVolume esetén ellenőrizni kell a StorageClass és a kötet Delete vagy Retain reclaim policy beállítását. A Delete policy a támogatott driver használatakor a háttértárolási erőforrást is törölheti, de a fizikai adatok Clear vagy Purge szintű kezelését a storage-szolgáltató dokumentációja és bizonyítéka alapján kell értékelni. Snapshotnál külön ellenőrizni kell a VolumeSnapshotClass törlési szabályát is.

Megosztott, thin-provisioned vagy deduplikált tárolón az UNMAP vagy Discard a blokkok felszabadítását jelezheti a háttértár felé, de önmagában nem igazolja a céladat biztonságos törlését. Az eredmény a mögöttes tárolórendszer blokkvisszanyerési és sanitize képességeitől függ.

Kriptográfiai törlés Purge technikaként akkor alkalmazható, ha:

- a törlendő virtuális lemezhez, kötethez vagy adatkörhöz megfelelően elkülönített kulcs vagy kulcshierarchia tartozik;
- valamennyi releváns másolat, snapshot, replika és mentés megfelelő titkosítással védett;
- a kulcstörlés nem érinti a megőrzendő adatokat;

- a végrehajtás és annak eredménye naplózható és igazolható.

A törlés csak akkor zárható le, ha a szervezet az aktív objektumok, snapshotok, persistent volume-ok, registry- és node-oldali példányok, mentések, valamint a kapcsolódó titkosítási kulcsok kezelését egyaránt ellenőrizte. Ha a logikai vagy kriptográfiai törlés hatóköre nem igazolható, a mögöttes dedikált adathordozót annak technológiájához igazodó Purge vagy Destroy eljárással kell kezelni.

1.2.7. Felhőszolgáltatások, objektumtárak és SaaS-rendszerek

Felhőszolgáltatás esetén a szervezet rendszerint nem fér hozzá közvetlenül a mögöttes fizikai adathordozókhoz. A törlési eljárást ezért a szolgáltatás logikai törlési funkciói, a szolgáltatói dokumentáció, a szerződéses vállalások, a naplózott műveletek alapján kell kialakítani.

A törlési hatókörnek a szolgáltatás képességei és az alkalmazandó megőrzési szabályok szerint ki kell terjednie:

- az aktív fájlokra, objektumokra és rekordokra;
- valamennyi korábbi verzióra;
- snapshotokra és replikákra;
- lomtár- és soft-delete példányokra;
- archivált és exportált másolatokra;
- szolgáltatói és ügyféloldali mentésekre;
- keresőindexekben, gyorsítótárakban, naplókban vagy analitikai rendszerekben létrejött releváns adatpéldányokra.

A naplók és auditadatok törlésénél figyelembe kell venni a biztonsági, jogszabályi és szerződéses megőrzési kötelezettségeket. Ha az azonnali törlés nem megengedett vagy műszakilag nem lehetséges, dokumentálni kell a megőrzés célját, időtartamát, védelmét és a végleges törlés időpontját.

A szolgáltatói törlési API vagy adminisztrációs funkció alkalmazása előtt ellenőrizni kell, hogy az adatokból maradtak-e korábbi verziók, soft-delete vagy lomtárban tárolt példányok, továbbá fennáll-e immutability, retention lock vagy legal hold korlátozás. Vizsgálni kell a replikációs, lifecycle- és backup-beállításokat, valamint azt is, hogy a szolgáltató milyen határidővel hajtja végre a végleges törlést.

Verziózott objektumtárban egy egyszerű törlési művelet gyakran csak törlési jelölőt hoz létre, vagy az aktuális verziót korábbi verzióvá alakítja. A korábbi verziókat külön kell eltávolítani, illetve lifecycle szabály útján törölni. Soft delete esetén az adat a megőrzési idő lejártáig helyreállítható maradhat.

Retention lock, immutability vagy legal hold alatt álló adatok a megőrzési idő lejártá vagy a zárolás jogszerű megszüntetése előtt jellemzően nem törölhetők. Ezeket az állapotokat már a törlési folyamat tervezésekor azonosítani kell, és a végleges törlés várható időpontját dokumentálni szükséges.

A szolgáltatói törlési művelet csak akkor tekinthető lezártnak, ha a szervezet ellenőrizte a törlési állapotot, az érintett verziókat és másolatokat, a megőrzési korlátozásokat, valamint a szolgáltató által vállalt végleges törlési határidőt. A fizikai adathordozók kezelését az ügyfél jellemzően nem tudja közvetlenül ellenőrizni, ezért annak megfelelőségét szerződéses vállalásokkal, szolgáltatói törlési dokumentációval és megfelelő assurance vagy auditbizonyítékokkal kell alátámasztani.

Felhőszolgáltató	Technikai naplók (Platform szintű bizonyítékok)	Megfelelőségi tanúsítványok (Assurance Reports)	Releváns szolgáltatói dokumentáció / Jogi garancia
Microsoft Azure	Azure Activity Logs (pl. Delete Storage Account, Delete Blob), Azure Resource Graph változásnaplók, Azure Purview adatkezelési naplók.	SOC 2 Type II, ISO 27001/27018 tanúsítványok (elérhető a <i>Service Trust Portal</i> felületén), amelyek igazolják a NIST 800-88 szerinti fizikai megsemmisítést.	Microsoft Data Protection Addendum (DPA), Azure szolgáltatási feltételek (megőrzési és törlési időablakok).
Amazon Web Services (AWS)	AWS CloudTrail naplók (pl. DeleteBucket, DeleteVolume), S3 Server Access Logs, Lifecycle szabályok végrehajtási naplói.	SOC 2 Type II Privacy & Security jelentések, ISO 27001/27017/27018 audit jelentések (letölthető az <i>AWS Artifact</i> portálról).	AWS Artifact biztonsági és megfelelőségi megállapodások, adattörlési SLA-k.
Google Cloud Platform (GCP)	Cloud Audit Logs (Admin Activity logs az adattörlési és erőforrás-megszüntetési eseményekről), Cloud Storage Object Lifecycle naplók.	SOC 2 Type II / SOC 3 jelentések, ISO 27001 és ISO 27701 tanúsítványok (elérhető a <i>Compliance Reports Manager</i> -en).	Google Cloud Data Processing Addendum (CDPA), biztonsági fehér könyvek (Security Whitepapers).
SaaS Platformok (pl. Microsoft 365, Google Workspace)	Microsoft 365 Unified Audit Log (megőrzési házirend és törlési események), Google Workspace Admin Audit Logs, eDiscovery audit naplók.	SaaS-specifikus SOC 2 Type II jelentések, BSI C5 (M365 esetén), ISO 27001/27701 felhőbiztonsági tanúsítások.	Szolgáltatói SLA-k a „soft-delete” és végleges törlési (hard delete) időszakokról, adatfeldolgozási megállapodások.

1. táblázat Néhány ismertebb felhő szolgáltató esetében az alábbi dokumentációval igazolhatjuk a törlés megfelelőségét

1.2.8. Biztonsági mentések és mágnesszalagok

A biztonsági mentések törlését a szervezet megőrzési szabályaival, helyreállítási követelményeivel, jogi megőrzési kötelezettségeivel és üzletmenet-folytonossági elvárásaival összehangoltan kell végrehajtani.

Mágnesszalag szervezeten belüli újra használata esetén a teljes rögzíthető tartomány felülírása Clear technika lehet. A műveletet a szalagmeghajtó gyártói eszközével, a backup-rendszer teljes médiatörlési funkciójával vagy más, a teljes szalag felülírására képes megoldással kell végrehajtani. A szalag gyors inicializálása vagy a címke újra írása nem jelent teljes felülírást.

Megfelelően méretezett és az adott szalagtípushoz igazolt degausserrel végzett demagnetizálás fizikai Purge technika lehet. A degausser kiválasztásánál ellenőrizni kell:

- a támogatott médiatípust;
- az alkalmazható maximális koercitást;
- a berendezés gyártói megfelelőségi adatait;
- a karbantartás vagy kalibrálás érvényességét;
- a ciklus sikerességének visszajelzését.

Titkosított backup esetén kriptográfiai törlés alkalmazható, ha a törlendő mentési generációkhoz elkülönített kulcs tartozik, a kulcs minden példánya megsemmisíthető, és a kulcstörlés nem tesz hozzáférhetetlenné még megőrzendő mentéseket. Egy több évnyi mentéshez vagy több ügyfélhez használt közös kulcs törlése nem megfelelően elkülönített törlési megoldás.

Hibás, részben olvasható vagy nem felülírható szalag esetén ellenőrzött fizikai megsemmisítést kell alkalmazni, például ipari aprítással, dezintegrálással vagy más, az alkalmazandó szabvány szerinti eljárással.

1.2.9. Optikai és analóg adathordozók

Újraírható optikai adathordozó szervezeten belüli, alacsonyabb kockázatú újra használata esetén a teljes írható területre kiterjedő törlés vagy felülírás Clear technikaként alkalmazható, ha a művelet sikeressége ellenőrizhető.

Nem újraírható optikai adathordozó esetén Destroy módszert kell alkalmazni. A megsemmisítés történhet:

- optikai adathordozók feldolgozására alkalmas, validált aprító- vagy dezintegráló berendezéssel;
- megfelelő maradványméretet biztosító granulálással vagy darálással;
- ellenőrzött ipari olvasztással vagy égetéssel;
- más, az alkalmazandó technikai szabványban elfogadott eljárással.

A megsemmisítésnek az adatrögzítő rétegre is ki kell terjednie. A lemez egyszerű megkarcolása, eltörése vagy egyetlen ponton történő átfúrása nem biztosít megfelelő eredményt.

Papíralapú dokumentumnál alkalmazható:

- az előírt maradványméretet biztosító iratmegsemmisítő;
- ipari aprítás vagy dezintegrálás;
- pépesítés;
- ellenőrzött ipari égetés.

A „keresztvágó” vagy „mikrovágó” megjelölés önmagában nem elegendő: igazolni kell, hogy a berendezés által előállított maradványméret megfelel az adatok bizalmasságához és az alkalmazott technikai szabványhoz meghatározott követelményeknek.

Az adathordozó látható sérülése vagy működésképtelensége önmagában nem bizonyítja a tárolt információ helyreállíthatatlanságát. A megsemmisítés eredményét a berendezés működése, a keletkezett maradványok és az előírt elfogadási kritériumok alapján ellenőrizni és validálni kell.

Külső megsemmisítési szolgáltató igénybevételekor zárt gyűjtést, dokumentált átadási és őrzési láncot, megfelelő tétel- vagy eszközazonosítást, valamint ellenőrizhető megsemmisítési igazolást kell biztosítani. Az igazolásnak lehetővé kell tennie, hogy minden átadott adathordozó egyedileg vagy megbízható tételszinten visszakövethető legyen.