Iktatószám: MNL/FOIG-T/11316-1/2023.

Magyar Nemzeti Levéltár

ARCHIVÁLÁSI SZABÁLYZAT

Dokumentum kontroll

Változások

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
1.0	2023.03.20	A Magyar Nemzeti Levéltár szerverein tárolt, keletkezett és kapott elektronikus adatok mentésére vonatkozó előírásokat, felelősségi köröket, valamint a feladatokat rögzíti.

Szabályozás elkészítéséért felelős

Verzió	Elfogadás dátuma	Beosztás	Név
1.0	2023.02.23	főosztályvezető	Bogár Anita

Szakmai tartalomért felelős szakterület

Verzió	Elfogadás dátuma	Beosztás	Név
1.0	2023.02.23	információbiztonsági vezető	Marx László

Nyilvántartás

Dokumentum kiadatásáért és nyilvántartásért felelős	Főigazgatói Titkárság Fazekas-Vincze Zsuzsanna titkárságvezető

Kiadás

Készült	2 eredeti példányban
Kapják	1. eredeti példány: Magyar Nemzeti Levéltár 2. eredeti példány: Elektronikus Ügyintézési Felügyelet Elektronikusan: a Magyar Nemzeti Levéltár honlapján nyilvánosan közzétéve

TARTALOMJEGYZÉK

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII.törvény (a továbbiakban: E-ügyintézési tv.), az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet, valamint az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet (a továbbiakban: Korm. rendelet) előírásainak figyelembevételével, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (1) bekezdés f) pontjában meghatározott feladatkörben, a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény 17. § (2) b) pontjába foglaltakra tekintettel, illetve a Magyar Nemzeti Levéltár (továbbiakban MNL) Szervezeti és Működési Szabályzata III. alcím 3. pont 1. alpont 5./f alpontjában rögzített hatáskörömben eljárva az MNL informatikai rendszereinek és információvagyonának mentésére, archiválására vonatkozó feladatokat, kötelezettségeket az alábbiak szerint szabályozom.[1]

1. Bevezetés

A szabályzat célja, hogy meghatározza az MNL E-ügyintézési tv. 25. § (4a) bekezdése szerinti, az ügyek intézésével kapcsolatos elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentési és archiválási folyamatainak részletszabályait.

Az adattrezor-archiválási kötelezettség célja az Adatkezelőnek az e-ügyintézési kötelezettség teljesítésével összefüggő adatai sérüléséből eredő működési zavara esetén a működési képesség helyreállítása és az adatvesztés minimalizálása.

Az MNL a szabályzat kereteinek megfelelően biztosítja az adatvédelemmel, az elektronikus ügyintézéssel, továbbá az adatok archiválásával összefüggő jogszabályi követelmények érvényesülését, így akadályozva meg az adatok bizalmasságának, sértetlenségének, valamint rendelkezésre állásának elvesztését. A szabályzat rendelkezései továbbá biztosítékot jelentenek arra, hogy az adatkezelő az e-ügyintézési kötelezettség teljesítésével összefüggő adatai sérüléséből eredő működési zavara esetén a működési képesség helyreállítására és az adatvesztés minimalizálására vonatkozó kötelezettségének eleget tegyen.

2. Általános rendelkezések

2.1. Alkalmazás

A szabályzat rendelkezéseit kell alkalmazni a Magyar Nemzeti Levéltár Hivatali Kapun, Hivatali Kapun (KÉR), Cégkapun és Ügyfélkapun történő ki- és bejövő megkeresésekre, az állampolgárokkal, az államigazgatási szervekkel, a helyi önkormányzatokkal, a közigazgatási hatósági és ítélkezési jogkör gyakorlására feljogosított jogalanyokkal folytatott elektronikus ügyintézés során.

Elektronikus információs rendszer megnevezése:

- Poszeidon (EKEIDR) elektronikus irat-és dokumentumkezelő rendszer

[1] A szabályzat az Elektronikus Ügyintézési Felügyelet által kibocsátott archiválás szabályzat minta figyelembe-vételével készült.

2.2. A szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed – adattrezor-archiválásra kötelezett adatkezelőként – az MNL munkavállalóira és az MNL részére adatfeldolgozó tevékenységet végző szerződéses partnerekre, függetlenül az adatfeldolgozás céljától és módjától.

2.3. A szabályzat tárgyi hatálya

A hatóságnak benyújtott elektronikus információs rendszereknek a köre.

2.4. A szabályzat időbeli hatálya

A jelen rendelkezés az aláírólapon megadott dátummal lép hatályba és visszavonásig marad hatályban.

2.5. Kapcsolódó szabályzatok, eljárások, rendelkezések

Jelen szabályzat alkalmazása során figyelemmel kell lenni különösen az MNL alábbi szabályzatainak rendelkezéseire:

a) MNL Informatikai Biztonsági Szabályzata

b) MNL Mentési eljárásrendje

c) MNL Információátadási Szabályzata

3. Értelmező rendelkezések

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

Adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

Adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

Adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

Archiválás: a nem, vagy nagyon ritkán használt, de megőrzendő adatok áthelyezése a feldolgozó rendszer tárolójáról egy másik, elkülönített tárolóra.

Archiválási eljárás: az archiválási stratégiát végrehajtó informatikai folyamat.

Archiválási szolgáltatás: az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás.

Archiválási politika: az archiválandó tartalomra vonatkozó szakmai elvárások, valamint az archivált adatok eléréséhez kapcsolódó szakmai követelmények meghatározása.

Archiválási stratégia: az archiválás alapvető szabályainak meghatározása, amely magában foglalja az archiválás tárgyát, módját, az archiválás személyi és tárgyi feltételeinek meghatározását, archiválási hardver, szoftver egység és szabálya azonosítását, az archiválás időpontját, ütemezését, megőrzési idejét.

Automatikus információátadás: információátadás az információ átadását biztosító együttműködő szerv részéről emberi beavatkozást nem igénylő módon.

Automatikus információátadási felület: az információ átadását biztosító együttműködő szerv által létrehozott és üzemeltetett, automatikus információátadást lehetővé tevő műszaki megoldás.

Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

EIR: elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese; Egy elektronikus információs rendszernek kell tekinteni adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

E-ügyintézési tv.: 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

Inkrementális mentés: nem kerül elmentésre minden kiválasztott elem, csak azok, amelyek a korábbi mentés óta változtak. Két alapvető típusa:

a) A **kumulatív mentés** során mindig az utolsó teljes mentés óta megváltozott adategységek kerülnek elmentésre.
b) A **differenciális mentés** során csak az utolsó inkrementális mentés óta megváltozott adategységek kerülnek elmentésre.

Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

Központi mentés: alapértelmezésben a mentések a rendszerbe állított központi mentőeszköz igénybevételével történnek.

Központi mentési eszköz: a szervezet adatbázisainak, alkalmazásainak, operációs rendszereinek és ezek környezetei mentési igényeinek végrehajtására rendszerbe állított nagyteljesítményű, megfelelő biztonsági megoldással és menedzsment felülettel rendelkező berendezés.

Kritikus szolgáltatás: informatikai szolgáltatás, amely a szervezet működése szempontjából létfontosságú.

Offline mentés: a mentés a szolgáltatások leállításával történik, a szolgáltatások a mentés ideje alatt nem érhetők el.

Online mentés: a mentés online módon, az informatikai szolgáltatás leállítása nélkül történik. A mentés ideje alatt az adott szolgáltatás elérhető, azonban lehetnek olyan funkciók, amelyek a mentés ideje alatt nem, vagy csak korlátozott mértékben vehetők igénybe.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

Tartós adathordozó: olyan eszköz, amely a címzett számára lehetővé teszi a neki címzett adatoknak az adat céljának megfelelő ideig történő tartós tárolását és a tárolt adatok változatlan formában és tartalommal történő megjelenítését. Ilyen eszköz különösen az USB kulcs, a CD-ROM, a DVD, a memória kártya, a számítógép merevlemeze.

Teljes (full) mentés: minden kiválasztott elem mentésre kerül.

Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

Visszaállítás: meghibásodás vagy sérülés miatt leállt informatikai szolgáltatás helyreállítása, amely megkívánhatja a rendszerek és adatbázisok mentéseinek visszatöltését. Katasztrófa-elhárítás esetén leginkább a gyors, ideiglenes szolgáltatás visszaállítást jelenti, megkülönböztetve a végleges helyreállítástól.

Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

4. Az archiválási folyamat résztvevői

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági és archiválási osztály-besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint az MNL ügyintézési ciklusával.

Az MNL Informatikai osztálya személyi állományának feladata a rendszeres és időszakos biztonsági mentések elvégzése. Azon információs rendszereknél, ahol az MNL adatfeldolgozót vesz igénybe, a mentés az adatfeldolgozó közreműködésével történik. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciája biztosítva legyen, illetve az egyéb munkaállomások hálózati munkáját ne akadályozza.

Az MNL informatikai rendszereire nézve a biztonsági másolatok készítésének, a mentések elvégzésének és tárolásának részletes rendjét az MNL Informatikai Biztonsági Szabályzata és a Mentési eljárásrend tartalmazzák.

Az archiválási folyamat során keletkező adatállományok kézbesítésére vonatkozó feladatokat az MNL által megbízott látja el a belföldi Állami Futárszolgálat tevékenységének szabályozásáról szóló 44/1998. (X. 14.) BM rendeletben foglaltaknak megfelelően.

5. Kockázatelemzés

Az MNL meghatározza az ügymenet folytonosság biztosításához szükséges szabályokat, követelményeket, amelynek érdekében:

a) Elkészíti a működés szempontjából jelentős informatikai szolgáltatások helyreállítási terveit.
b) A fontos informatikai szolgáltatások meghatározásához kockázatelemzést végez.
c) Az azonosított szolgáltatásoknál:
- megvizsgálja a kulcsfontosságú elemeket;
- meghatározza a még tolerálható helyreállítási időket;
- elkészíti a helyreállítási terveket;
- azokat a gyakorlatban is teszteli.

A szabályokat és követelményeket tartalmazó dokumentumok előkészítését és a kockázatelemzést az informatikai osztály és az integrált kockázatkezelési rendszer koordinálására kijelölt szervezeti felelős végzi el.

5.1. Internet kapcsolat (WAN — World Area Network) kiesése

Működésfolytonosság (BCP):

Hatása az ügymenetre: kritikus (telephelyek nem érik el a központi szervert és valamennyi felhőalapú rendszer elérhetetlenné válik).

Valószínűsége: magas rendelkezésre állás miatt évente 1 alkalom.

Helyreállítási idő: legfeljebb 12 óra.

Kockázatkezelés:

Az esetet a szolgáltatónál be kell jelenteni. [A szerződésben törekedni kell arra, hogy az SLA (Service Level Agreement) alapú legyen, azaz a szolgáltatás minőségétől függ a szolgáltatási díj és legalább 99,5 %-os rendelkezésre állást biztosítson.]

Helyreállítás (DRP):

- fővonal hiba esetén: Az esetet a szolgáltatónak haladéktalanul be kell jelenteni;

- router/modem hiba esetén: Funkcionális csereeszköz haladéktalan igénylése a szolgáltatótól.

5.2. Belső hálózat (LAN — Local Area Network) elemeinek meghibásodása

Működésfolytonosság (BCP):

Hatása az ügymenetre: kritikus (minden szerveren tárolt dokumentum és onnan futó szolgáltatás, illetve minden felhő alapú szakalkalmazás elérhetetlenné válik a belső hálózatból).

Valószínűsége: évente egyszer.

Helyreállítási idő: legfeljebb 4 óra

Kockázatkezelés:

Jó minőségű hálózati eszközök és legalább CAT5 minőségű kábelezés alkalmazása, hálózati szolgáltató bevonása magas SLA-val. Rendszeres karbantartással, teszteléssel jelentősen csökkenthető a meghibásodás valószínűsége. Meghibásodás esetén a hibás eszközök azonnali cseréje.

Helyreállítás (DRP):

- Aktív elem meghibásodása esetén:
  - hibabehatárolás;
  - a hiba jelentése a szolgáltatónak;
  - funkcionális csereeszköz leszállítása, beállítása és konfigurálása;
  - tesztelés;
  - próbaüzem;
  - éles üzem;
  - dokumentálás.
- Passzív elem (kábel, rack, stb.) meghibásodása esetén:
  - hibabehatárolás;
  - a hiba jelentése, az érintettek tájékoztatása;
  - a passzív szakasz, vagy alkatrész cseréje;
  - tesztelés;
  - dokumentálás.

5.3. Csoportmunka szerver (fájl szerver) meghibásodása

Működésfolytonosság (BCP):

Hatása az ügymenetre: kritikus (minden szerveren tárolt dokumentum és onnan futó szolgáltatás elérhetetlenné válik).

Valószínűsége: háromévente egyszer.

Helyreállítási idő: kb. 24 óra.

Kockázatkezelés:

- karbantartási szerződés a szerver komponensek szállítóival;
- jó minőségű alkatrészek alkalmazása, valamint a bizonytalanok cseréje;
- legalább RAID 5 adattárolás szükséges;

- adatbázisok mentése napi gyakorisággal;
- fájlstruktúra mentése napi gyakorisággal;
- rendszernapló állományok folyamatos mentése, elemzése és annak dokumentálása;
- meghibásodás esetén a hibás alkatrész azonnali cseréje;
- szükség szerint újratelepítés, adatbázis adatok betöltése;
- tesztelés és üzembe helyezés.

Helyreállítás (DRP):

Alkatrész (alaplap, CPU, memória, HDD, táp) meghibásodása esetén:

- hibabehatárolás;
- a hiba jelentése a szerződéses szolgáltatónak, az MNL vezetőinek tájékoztatása;
- adatok lemásolása egy másik eszközön;
- hibátlannak gondolt elemek tesztelése egy működő környezetben;
- csere alkatrészek beépítése, vagy pótlása funkcionálisan megfelelővel;
- szükség esetén OS újratelepítése;
- konfigurálás a kötelező konfigurációs beállítások listája szerint;
- tesztelés;
- szükség szerint az adatok visszamásolása;
- próbaüzem;
- éles üzem.

6. Az archiválás folyamata

A mentési, archiválási rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőből adódó hibák előfordulásának valószínűségét.

Törekedni kell arra, hogy a mentések tárolása fizikailag biztonságos legyen, védeni kell őket az illetéktelen hozzáférésektől, illetve a különböző fizikai behatásoktól (tűz, víz stb.).

A központi szervereken tárolt elektronikus információvagyont a biztonsági káresemények ellen szintén mentéssel kell védeni. A mentéseket minden mentési rendet érintő (fizikai, logikai, vagy adminisztratív) változáskor, de legalább évente egyszer ellenőrizni kell aszerint, hogy visszatöltésük, helyreállításuk valóban működik-e. Az ellenőrzéseket dokumentált módon kell végrehajtani.

A szervezet 2.1. pontban megnevezett információs rendszere a 4-es biztonsági osztályba került besorolásba.

A 4-es kategóriába sorolt rendszerről első alkalommal, valamint legalább három havonta teljes adatállomány archiválás történik, továbbá archiválás történik havonta a változásokról.

6.1. Az archiválási folyamat főbb szakaszai

Az archiválási folyamat négy jól elkülöníthető szakaszra bontható:

- az érintett EIR adatállományainak kijelölése és titkosított mentése az adatmennyiségtől függő kapacitású LTO kazettára;
- a mentés ellenőrzése;

- az érintett EIR futtató környezetének teljes mentése tartós adattárolóra (mérettől függően CD, DVD, LTO kazettára), amennyiben szükséges;
- a titkosított adathordozó eljuttatása a Kormányzati Adattrezorba.

A felsorolt feladatokat az MNL Informatikai Osztálya rendszergazdája végzi, a kazetta adattrezorba juttatását az MNL megbízottja végzi.

A futtatási környezet archiválásakor az EIR architektúrájának leírását, teljes dokumentációját is el kell archiválni. Minden verzióváltás után kötelező a teljes dokumentáció archiválása. A dokumentációnak tartalmaznia kell az esetleges fejlesztési környezetet is, hogy reprodukálható legyen a rendszer.

7. A tárolt és mentésre kerülő adatok köre

Az MNL az elektronikus ügyintézés keretében nyújtandó szolgáltatásai biztosítása, valamint ügyviteli feladatai ellátása érdekében elektronikus iratkezelési rendszert működtet, megnevezése:

Poszeidon (EKEIDR) elektronikus iratkezelő rendszer, melyben az MNL-nek, mint adatkezelőnek a Hivatali Kapu, Hivatali Kapu (KÉR), Cégkapu és Ügyfélkapu szolgáltatásokon keresztül keletkezett ki- és bejövő adatai, dokumentumai kerülnek iktatásra.

Az elektronikus ügyintézés keretében keletkező iratok iktatása és archiválása során az alábbi adatok kerülnek rögzítésre, illetve tárolásra:

- irat beérkezés dátuma (érkeztetés, iktatás időpontja);
- érkeztetési azonosító;
- küldő fél megnevezése, azonosító adatai (KRID);
- iktatószám vagy érkeztetési azonosító;
- irat kiküldésének dátuma;
- fogadó fél megnevezése, azonosító adatai (KRID);
- feladási értesítő;
- a be- és kimenő irat, valamint mellékletei, függelékei.

Az elektronikus formában kezelt adatok bizalmasságának és sértetlenségének biztosítását célzó intézkedéseket az MNL a Nemzeti Kibervédelmi Intézet sérülékenységvizsgálatát követő intézkedési tervében fogalmazta meg és hajtotta végre.

8. Hatósági ellenőrzés

Az Elektronikus Ügyintézési Felügyelet eljárásának részletes szabályait, valamint a felügyeleti vizsgálat részletes szabályait az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII.19.) Korm. Rendelet (Vhr.), TrezorR. 12. § (5)-(8), 13. §, 14 § (1), (2), 17 § (1) bekezdési szabályozzák.

Kapcsolattartás: Az archiválásra kötelezettek az archiválási szabályzataikat az Elektronikus Ügyintézési Felügyelet hivatali kapu címére küldhetik meg. Hivatali kapu cím: EUF.

9. Tesztelés

Az archív állományok ellenőrzése céljából tesztelési tervet kell készíteni, amely az alábbiakat tartalmazza:

- az elektronikus információs rendszer környezetére (OS, adatbáziskezelő stb.);
- milyen időközönként történik;
- eredmények dokumentálásának módja, kiértékelése, írásban rögzítése, amely alkalmas arra; hogy a hatóságnak be lehessen mutatni.

10. Záró rendelkezések

Jelen szabályzatban foglaltak az aláírás napján lépnek hatályba.

Budapest, az elektronikus aláíráson jelzett dátum szerint.

MAGYAR NEMZETI LEVÉLTÁR főigazgató

Szabó Csaba
2023.03.20
08:38:27 +01'00'

Dr. habil Szabó Csaba

főigazgató

Mellékletek, függelékek

1. sz. melléklet Archiválási osztály elemzési tábla

Külön MS excelben.
Archiválási_Osztály_Elemzés_Poszeidon.xlsx

2. sz. melléklet Archiválási osztály összesítő tábla

Külön MS excelben.
Archiválási osztály összesítö_.xlsx