Archiválási szabályzat

/módosításokkal egységes szerkezetben/

Dr. Papp IstvánAndrás Végrehajtói Irodája

Verziószám: 1.0

Készítette: Dr. Papp István András

Jóváhagyta: Dr. Papp István András

Dokumentum kontroll

Változások

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
v1.0	2019.06.14.	Dr. Papp István András Végrehajtói Irodája archiválási szabályzatának elkészítése

Szabályozás elkészítéséért felelős

Verzió	Elfogadás dátuma	Beosztás	Név
v1.0	2019.06.17.	megbízott adatvédelmi tisztviselő	Dr. Papp István András

Szakmai tartalomért felelős szakterület

Verzió	Elfogadás dátuma	Beosztás	Név
v1.0	2019.06.17.	megbízott rendszergazda	Kelemen Zsuzsanna

Nyilvántartás

Dokumentum kiadatásáért és nyilvántartásért felelős	Dr. Papp István András

Kiadás

Készült	1 eredeti példányban
Kapják	1. eredeti példány: Irattár Elektronikusan: • Elektronikus Ügyintézési Felület

Tartalomjegyzék

Bevezetés

Dr. Papp István András Végrehajtói Irodája *(továbbiakban: Végrehajtói Iroda) jelen archiválási szabályzatának célja az önálló bírósági végrehajtói tevékenység teljesítése során az Egységes Végrehajtói Ügyviteli Rendszer működési zavara esetén, a működési képesség helyreállítása és az adatvesztés minimalizálása a 466/2017. (XII.28.) Korm. rendelettel, valamint a Végrehajtói Iroda belső szabályzataival és előírásaival összhangban.*

Jelen archiválási szabályzattal a Végrehajtói Iroda meghatározza az adattrezori-archiválási kötelezettség szerinti, az ügyek intézésével kapcsolatos elektronikus információs rendszerében és nyilvántartásában tárolt nem minősített archiválásra és biztonsági mentésére vonatkozó feladatait és kötelező szabályait.

Általános rendelkezések

Alkalmazás

A szabályzat rendelkezései a Végrehajtói Iroda Egységes Végrehajtói Ügyviteli Rendszeréhez kapcsolódó minden informatikai rendszer esetében jelen szabályzatban részletezett módon teljes körűen alkalmazni kell.

A szabályzat személyi hatálya

Az archiválási szabályzat személyi hatálya kiterjed valamennyi, a Végrehajtói Irodával teljes vagy részmunkaidős munkaviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban álló személyre, valamint – ha van ilyen – a mentési-archiválási folyamatban résztvevő, illetve azt szerződés alapján végző harmadik személyekre is.

A szabályzat tárgyi hatálya

Jelen szabályzat hatálya kiterjed a Végrehajtói Iroda által kezelt, jogszabályi védelmet élvező adatok teljes körére, az Egységes Végrehajtói Ügyviteli Rendszerben tárolt adatokra.

A szabályzat időbeli hatálya

Visszavonásig.

Kapcsolódó szabályzatok, eljárások, rendelkezések

Kapcsolódó szabályzat a Végrehajtói Iroda Adatvédelmi Szabályzata és Informatikai Biztonsági Szabályzata.

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

Az archiválási folyamat résztvevői

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, a 466/2017. (XII. 28.) Korm. rendelet 1. melléklet szerinti biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Végrehajtói Iroda ügyintézési ciklusával. A rendszergazda feladata a rendszeres és időszakos biztonsági mentések elvégzése. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciája biztosítva legyen, illetve az egyéb munkaállomások hálózati munkáját ne akadályozza.

A Végrehajtói Iroda informatikai működéséhez szükséges informatikai, adminisztratív, fizikai és humán erőforrások: megbízott rendszergazda, irodavezető, végrehajtási ügyintézők.

Kockázatelemzés

A Végrehajtói Iroda meghatározza az ügymenet folytonosságának biztosításához szükséges szabályokat, követelményeket:

- El kell készíteni a működés szempontjából jelentős informatikai szolgáltatások helyreállítási terveit.
- A fontos informatikai szolgáltatások meghatározásához kockázatelemzést kell végezni.
- Az azonosított szolgáltatásoknál
    - meg kell vizsgálni a kulcsfontosságú elemeket,
    - meg kell határozni a még tolerálható helyreállítási időket
    - el kell készíteni a helyreállítási terveket és
    - azokat a gyakorlatban is tesztelni kell.

Internet kapcsolat (WAN — World Area Network) kiesése

Működésfolytonosság (BCP):

Hatása az ügymenetre: lényeges (az elektronikus kapcsolattartás 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 99,5 %-os rendelkezésre állást biztosítson.]

Helyreállítás (DRP):

- Fővonal hiba esetén: Az esetet az szolgáltatónál történő haladéktalan bejelentése.

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

Belső hálózat (LAN — Local Area Network) elemeinek meghibásodása

Működésfolytonosság (BCP):

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

Valószínűsége: évente egyszer

Helyreállítási idő: legfeljebb 4 óra

Kockázatkezelés: Jó minőségű hálózati eszközök és legalább CAT5 minőségű kábelezés alkalmazása,valamint a bizonytalan elemek cseréje. 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, az érintettek tájékoztatása.
    - Funkcionális csereeszköz 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
    - Próbaüzem
    - Dokumentálás
    - Éles üzem
    - Dokumentálás

Csoportmunka szerver (fájl szerver), adatbázisszerver meghibásodása

Működésfolytonosság (RCP):

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

Valószínűsége: három évente egyszer.

Helyreállítási idő: kb. 24 óra.

Kockázatkezelés:

- Jó minőségű alkatrészek alkalmazása, valamint a bizonytalanok cseréje.
- Rendszeres karbantartással jelentősen csökkenthető a meghibásodás valószínűsége.
- Legalább RAID 1 tükrözés szükséges.
- Adatbázis mentése napi gyakorisággal.
- Rendszernapló állományok folyamatos elemzése és annak dokumentálása.
- Meghibásodás esetén a hibás alkatrész azonnali cseréje.
- Szükség szerint újratelepítés. Adatbázis adatok betöltése.
- Tesztelés és üzembe helyezés.

Helyreállítás (DRP):

- Alaplap meghibásodása esetén:
    - Hibabehatárolás
    - A hiba jelentése, az érintettek tájékoztatása.
    - Adatok lemásolása egy másik eszközön

- Hibátlannak gondolt elemek tesztelése egy működő környezetben
- Hibátlannak bizonyult elemek visszaépítése, vagy pótlása funkcionálisan megfelelővel
- OS újratelepítés
- Konfigurálás a kötelező konfigurációs beállítások listája szerint
- Tesztelés
- Szükség szerint az adatok visszamásolása
- Próbaüzem
- Éles üzem

- Háttértár meghibásodás esetén (HDD, SSD):
  - Hibabehatárolás
  - A hiba jelentése, az érintettek tájékoztatása
  - Alkatrészcsere a funkcionálisan megfelelő, vagy erősebb alkatrészre
  - Adatok lemásolása egy másik eszközön — ha szükséges külső szervizben
  - Hibátlannak gondolt elemek tesztelése egy működő környezetben
  - Hibátlannak bizonyult elemek visszaépítése, vagy pótlása funkcionálisan megfelelővel
  - Szükség szerint OS újratelepítés.
  - Konfigurálás a kötelező konfigurációs beállítások listája szerint
  - Tesztelés
  - Szükség szerint az adatok visszamásolása
  - Próbaüzem
  - Éles üzem

- Alkatrész meghibásodás esetén (CPU, memória, hűtés, táp, illesztő kártyák):
  - Hibabehatárolás
  - A hiba jelentése, az érintettek tájékoztatása
  - Alkatrészcsere a funkcionálisan megfelelő, vagy erősebb alkatrészre
  - Adatok lemásolása egy másik eszközön
  - Hibátlannak gondolt elemek tesztelése egy működő környezetben
  - Hibátlannak bizonyult elemek visszaépítése, vagy pótlása funkcionálisan megfelelővel
  - Szükség szerint OS újratelepítés
  - Konfigurálás a kötelező konfigurációs beállítások listája szerint
  - Tesztelés
  - Szükség szerint az adatok visszamásolása
  - Próbaüzem
  - Éles üzem
  - 3 nap kiemelt felügyelet

Az archiválás folyamata

A Végrehajtói Iroda információs rendszere és nyilvántartása 466/2017. (XII. 28.) Korm. rendelet 1. melléklet szerinti besorolása: 5-ös kategória.

Az információs rendszerek és nyilvántartások besorolásának megfelelően a rendszerről első alkalommal, valamint évente a teljes állomány archiválásra kerül.

Érintett rendszer:

- **EVÜR (Egységes Végrehajtói Ügyviteli Rendszer)**

Az emberi tényezőből adódó hibák elkerülése érdekében kívánatos a lehető legnagyobb mértékű automatizálást megvalósítani a mentési, archiválási rendszer vonatkozásában.

Amennyiben ez nem lehetséges, az adatok archiválásáért felelős személy a megbízott rendszergazda.

A mentéseknek ki kell terjednie a működési folyamatok és tevékenységek támogatásában és kiszolgálásában részt vevő informatikai eszközökre, illetve azok elhelyezésére szolgáló létesítményekre; az archivált EIR futtatási környezetét, architektúrájának leírását, teljes dokumentációját el kell archiválni a rendszer reprodukálhatóságának érdekében. Minden verzióváltás után a teljes dokumentáció archiválásra kerül.

Az archiválást, a biztonsági mentést külön-külön erre a célra fenntartott, hordozható adathordozókon kell tárolni. Az adathordozókat a mentést, illetve archiválást követően az adatokat rendszerszerűen tároló információs rendszertől, illetve nyilvántartástól eltérő helyiségben, külön elzárva kell tárolni. Az elhelyezett adattárolót óvni kell bármely, az adatok épségét veszélyeztető külső behatástól, így különösen a jogosulatlan hozzáféréstől, valamint a különböző fizikai behatásoktól. Ennek érdekében az adathordozókat lehetőleg külön, erre a célra rendszeresített biztonsági szekrényekben kell elhelyezni. Az archiválást, illetve a biztonsági mentést tartalmazó adattárolók típusa: külső HDD

A Végrehajtói Iroda az archiválási szabályzat által elérni kívánt célok biztosítása érdekében a biztonsági mentéseket minden, a mentési rendet jelentősen befolyásoló változás alkalmával, de legalább évente teljes körűen köteles ellenőrizni, hogy visszatöltésük, helyreállításuk valóban működik-e. Az ellenőrzéseket dokumentálni kell, arról elektronikus vagy papír alapú jegyzőkönyvet kell készíteni.

Az adatkezelő köteles kijelölni a szervernek azon területét, melyen a felhasználók az archiválás, illetve a biztonsági mentés által nem érintett, munkájuk szempontjából azonban fontos dokumentumokat tárolják.

Az archiválási folyamat főbb szakaszai:

a. az érintett adatállomány kijelölése és mentése az adatmennyiségtől függő típusú tartós adathordozóra, illetve ennek ellenőrzése,
b. a mentett adatokat tartalmazó adathordozó titkosítása,
c. a titkosított adathordozó átadása az őrzésért felelős NISZ Zrt. felé, egyúttal az adathordozó NISZ Zrt. általi átvétele.

A tárolt és mentésre kerülő adatok köre

Az Elektronikus Információs Rendszer neve	**EIR rövid kódja**	**EIR állapota**
Egységes Végrehajtói Ügyviteli Rendszer	EVÜR	aktív

Az EVÜR -ben tárolt adatok:

- a végrehajtási ügyek ügyszáma, végrehajtható okirat száma, bírósági határozat számai;
- végrehajtási eljárásban résztvevő jogi személyek, természetes személyek személyes adatai, címei, elérhetőségei;
- végrehajtási eljárás adósának fellelt vagyonának adatai (ingó-ingatlan megnevezés, címe, értéke; munkahely neve, címe; bankszámlaszámai);
- valamint a végrehajtási eljárások pénzügyi nyilvántartása.

Hatósági ellenőrzés

Az archiválási szabályzatban meghatározott információs rendszerek archiválása az osztályba sorolást követően az előírt gyakorisággal történnek.

Az archiválások gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Végrehajtói Iroda ügyintézési ciklusával.

Kapcsolattartás:

Az archiválási folyamat résztvevői által történik, Hivatali Kapun keresztül.

Tesztelés

A Végrehajtói Iroda az archív állományokat és a biztonsági mentéseket minden, az archiválási és mentésirendet jelentősen befolyásoló változás alkalmával, de legalább évente köteles ellenőrizni, hogy visszatöltésük, helyreállításuk valóban működik-e. Az ellenőrzés folyamatát és azok eredményét dokumentálni kell, arról elektronikus vagy papír alapú jegyzőkönyvet kell készíteni olyan formátumban, mely alkalmas arra, hogy azokat a hatóságnak be lehessen mutatni.

A fentieken túl az állományok megfelelőségét (archívumok helyreállíthatósága, biztonsági mentések felhasználthatósága), valamint az elektronikus információs rendszer környezetére (operációs rendszer adatbázis kezelő, futtatási környezet stb.) szúrópróbaszerűen tesztelni kell, illetve automatikus ellenőrzéseket kell végrehajtani.

Ennek betartásáért a biztonsági mentés elvégzésével megbízott rendszergazda tartozik felelősséggel. A tesztek lefolytatását szintén dokumentálni kell, azzal, hogy sikertelen mentés esetén haladéktalanul, a lehető legrövidebb időn belül meg kell ismételni a mentési eljárást.