Archiválási szabályzat

dr. Kőszegi Károly Végrehajtói Irodája

Verziószám: v1.0

Változások

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
v1.0	2023.01.01	Archiválási Szabályzat elkészítése

Szabályozás elkészítéséért felelős

Verzió	Elfogadás dátuma	Beosztás	Név
v1.0	2023.01.01	önálló bírósági végrehajtó	dr. Kőszegi Károly

Szakmai tartalomért felelős szakterület

Verzió	Elfogadás dátuma	Beosztás	Név
v1.0	2023.01.01	rendszergazda	[redacted]

Nyilvántartás

Dokumentum kiadatásáért és nyilvántartásért felelős	dr. Kőszegi Károly

Kiadás

Készült	2 eredeti példányban
Kapják	2. eredeti példány: Végrehajtói Iroda nyilvántartásában Elektronikusan: megküldve az Elektronikus Ügyintézési Felügyeleti Hatóság részére

Tartalomjegyzék

Bevezetés

dr. Kőszegi Károly Végrehajtói Irodája szabályzatának célja az e-ügyintézési kötelezettség teljesítésével összefüggő, adatok sérüléséből adódó működési zavar esetén, a működési képesség helyreállítása és az adatvesztés minimalizálása a vonatkozó jogszabályokkal (2015. évi CCXXII törvény, 466/2017. (XII. 28.) Korm. rendelet, 910/2014/EU- rendelet), a szervezet belső rendelkezéseivel összhangban. Meghatározza a szervezet informatikai rendszereinek és információvagyonának mentését, archiválását, feladatokat, kötelező szabályokat.

Általános rendelkezések

Alkalmazás

A szervezet informatikai rendszereiben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell.

A biztonsági mentések mellett archiválást kell végezni az elektronikus ügyintézéssel összefüggő, a szervezet által saját szoftverkörnyezetben kezelt adatok tekintetében. Az archiválást olyan formátumban kell elvégezni, hogy abból értelmezhető adatot csak az adatkezelő, és csak az archiválás visszaállítását követően tudjon előállítani. Ha az archiválási kötelezettséggel érintett nyilvántartások esetén az adatok visszaállítása aránytalanul költséges vagy időigényes, az adattrezor archiválásnak az adatokkal együtt a futtatási környezetet is tartalmaznia kell. Az adattrezor archiválásnak tartalmaznia kell a visszaállításhoz szükséges dokumentációt is.

A szabályzat személyi hatálya

Az archiválási szabályzat személyi hatálya a szervezet valamennyi teljes vagy részmunkaidős, valamint szerződéses dolgozójára kiterjed. Kiterjed a Szervezet archiválási, mentési eljárásaiban résztvevő szerződéses partnerekre.

A szabályzat tárgyi hatálya

Adattárház archiválási kötelezettség tárgyi hatálya az E-ügyintézési tv. 25. § (4a) bekezdése szerinti, az elektronikus ügyintézést biztosító szervnek az ügyek intézésével kapcsolatos, elektronikus információs rendszereiben és nyilvántartásaiban tárolt, nem minősített adatai biztonsági mentési állományaira terjed ki. Ennek megfelelően az archiválási, és adattrezor archiválási rend az Adatkezelő vonatkozásában kiterjed a Nyilvántartás egészére, azaz az EVÜR-ben nyilvántartott adatokra, és – amennyiben az EVÜR eltér az MBVK által a végrehajtók részére biztosított alkalmazás verziótól (aktuális verzió elérhető itt: [redacted]evur=465214b7410 [redacted] vagy a Nyilvántartás vezetésére kialakított informatikai szoftver infrastruktúra tartalmaz nem az MBVK által biztosított elemeket is– ezen további alkalmazások, beépülő elemek adattartalmára és futtatási környezetére (ideértve a csatlakozó valamennyi szoftveres kiegészítő modult, az abban tárolt állományokat, és a kiegészítő szoftveres modul telepítéséhez szükséges valamennyi adatot). Az archiválandó tartalom mentésekor az EVÜR működéséhez szükséges valamennyi állomány és az EVÜR-ben fellelhető valamennyi adat mentése szükséges.

Az archiválási szabályzat tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére
- a Szervezet számítógépes hálózatára és annak elemeire
- az e-ügyintézéshez kapcsolódó informatikai rendszerekre
- jogosultságot kezelő gépekre

A szabályzat időbeli hatálya

Az archiválási szabályzatot évente, vagy jelentősebb infrastrukturális változás, illetve jogszabály változás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell!

Kapcsolódó szabályzatok, eljárások, rendelkezések

1/2002. (I. 17.) IM rendelet a bírósági végrehajtási ügyvitelről és pénzkezelésről 46.§. (3) alapján „A számítógépen tárolt adatokat naponta 2 példányban számítástechnikai adathordozóra kell menteni, és a 2 példányt egymástól elkülönítve, az adatok eredeti tárolási helyétől eltérő helyeken kell tárolni."

A Vüsz 18.§, 22/C. §, 28/A. §, 46.§ (3), (5) alapján az önálló bírósági végrehajtó köteles:

- a hozzá érkezett végrehajtási ügyet köteles érkezési sorrendben a végrehajtási ügyek számítógépes nyilvántartásába (a továbbiakban: Nyilvántartás) bejegyezni;
- a végrehajtási ügyet a Nyilvántartásban mindaddig nyilvántartásban tartani, amíg a végrehajtási ügy iratai nem selejtezhetők,
- az általa intézett bírósági végrehajtási ügyekben és a Vüsz. 1. § (2) bekezdése szerinti ügyekben az eljárása során keletkezett iratokat, utóiratokat, tértivevényeket az ügyiratokba történő beszerelés és az ügyiratokban történő nyilvántartás mellett digitalizálni és archiválni,
- az iratokat a beérkezésüket követő 15 napon belül digitalizálni, majd a végrehajtási ügy befejezését követő 15 napon belül archiválni,
- az elektronikus intézkedéseket tartalmazó elektronikus dokumentumok őrzésére a végrehajtási ügyek irataira vonatkozó irattári szabályokat megfelelően alkalmazni,
- a Nyilvántartásban tárolt adatokat naponta 2 példányban számítástechnikai adathordozóra menteni, és a 2 példányt egymástól elkülönítve, az adatok eredeti tárolási helyétől eltérő helyeken kell tárolni,
- ügyviteli, irat- és pénzkezelési feladatokat a Magyar Bírósági Végrehajtói Kar (a továbbiakban: MBVK) e célból létrehozott és a végrehajtó részére biztosított EVÜR alkalmazás igénybevételével végezni.

Jelen szabályzat alkalmazása során Adatkezelőnek az önálló bírósági végrehajtó minősül. Az archiválási kötelezettség teljesítése során az végrehajtói iroda adatfeldolgozóként biztosítja részére a folyamatok technikai végrehajtását.

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, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Szervezet ügyintézési ciklusával. A Szervezet megbízott dolgozójának feladata a rendszeres és időszakos biztonsági mentések elvégzése. Azon információs rendszereknél, ahol a szervezet 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.

Kockázatelemzés

A Szervezet meghatározza az ügymenet folytonosság (azaz, hogy az informatikai rendszerek folytatni tudják működésüket az elvárt és egyeztetett időn belül) biztosításához szükséges, szabályokat, követelményeket:

- Ehhez el kell készíteni az fontos 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:	kritikus (valamennyi internet elérésű rendszer elérhetetlenné válik, Pl. JÜB, TAKARNET, Ügyfélkapu, E-cégjegyzék, VIEKR, stb.)
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 a szolgáltatónál haladéktalanul be kell jelenteni.
- 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, illetve minden internet alapú alkalmazás elérhetetlenné válik a belső hálózatból)
Valószínűsége:	évente 1 alkalom
Helyreállítási idő:	legfeljebb 6 óra.

Kockázatkezelés:

- Jó minőségű hálózati eszközök és legalább CAT5 minőségű kábelezés alkalmazása. 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
  - Éles üzem
  - Dokumentálás

Központi szerver meghibásodása

Működésfolytonosság (BCP):

Hatása az ügymenetre:	kritikus (minden szerveren tárolt dokumentum és onnan futó szolgáltatás elérhetetlenné válik)
Valószínűsége:	5 évente 1 alkalom
Helyreállítási idő:	24 óra.

Kockázatkezelés:

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

Helyreállítás (DRP):

- Alaplap meghibásodása esetén
  - Hibabehatárolás
  - A hiba jelentése, az érintettek tájékoztatása.
  - Adatok mentése.
  - Elemek tesztelése egy működő környezetben.
  - Hibátlan elemek visszaépítése
  - OS újratelepítése.
  - Konfigurálás
  - Tesztelés
  - Szükséges adatok visszamásolása
  - Próbaüzem
  - Éles üzem
  - Dokumentálás
  - 3 nap kiemelt felügyelet

- Háttértár (HDD, SSD) meghibásodása esetén
  - Hibabehatárolás
  - A hiba jelentése, az érintettek tájékoztatása.
  - Alkatrészcsere a funkcionálisan megfelelő, vagy erősebb alkatrészre
  - Adatok mentése, ha szükséges külső szervizben.
  - Elemek tesztelése egy működő környezetben.
  - Hibátlan elemek visszaépítése
  - OS újratelepítése.
  - Konfigurálás
  - Tesztelés
  - Szükséges adatok visszamásolása
  - Próbaüzem
  - Éles üzem
  - Dokumentálás
  - 3 nap kiemelt felügyelet

- Alkatrész meghibásodás esetén (CPU, memória, hűtés, táp, illesztő kártyák) meghibásodása esetén:
  - Hibabehatárolás
  - A hiba jelentése, az érintettek tájékoztatása.
  - Alkatrészcsere a funkcionálisan megfelelő, vagy erősebb alkatrészre
  - Adatok mentése, ha szükséges külső szervizben.
  - Elemek tesztelése egy működő környezetben.
  - Hibátlan elemek visszaépítése
  - OS újratelepítése.
  - Konfigurálás
  - Tesztelés
  - Szükséges adatok visszamásolása
  - Próbaüzem
  - Éles üzem
  - Dokumentálás
  - 3 nap kiemelt felügyelet

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. A mentéseknek ki kell terjednie a működési folyamatok és tevékenységek támogatásában és kiszolgálásában részt vevő informatikai eszközökre, illetve azok elhelyezésére szolgáló létesítményekre.

A mentést, archiválást követően az adathordozót a szerver szobától eltérő helyiségben (ajánlott a szerverszobával nem azonos épületben), erre a célra rendszeresített biztonsági szekrényben, elzárva kell tárolni. 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 mentéseket a szerverektől elkülönítve, legalább külön helyiségben kell tárolni, védve mind a különböző fizikai káreseményektől (tűz, csőtörés-vízbetörés, stb.), mind az illetéktelen hozzáféréstől (lopás, illegális másolás).

A felhasználók munkaállomásokon lévő adatai nem kerülnek mentésre, ezért a felhasználók a munkájukhoz tartozó fontos dokumentumokat a fájlszerverek megfelelő kijelölt területein kötelesek tárolni!

A szervezet információs rendszerei 1-es kategóriába kerültek besorolásba, amely szerint a rendszerekről első alkalommal, valamint legalább évente teljes adatállomány archiválás történik. Archiválás történik havonta a változásokról.

Érintett rendszerek

Sorsz.	Az Elektronikus Információs rendszer neve	EIR rövid kódja	osztály
1	Egységes Végrehajtói Ügyviteli Rendszer	EVÜR	1

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 Szervezet ügyintézési ciklusával.

Tesztelés

A biztonsági mentéseket hibajelzés-mentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szúrópróba szerűen tesztelni kell, illetve automatikus ellenőrzéseket kell végrehajtani. Ennek betartásáért a biztonsági mentés

elvégzésével megbízott munkatárs, illetve a megbízott rendszergazda tartozik felelősséggel. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

A tesztelések elvégzésének menetét, eredményét dokumentálni kell!

Mellékletek, függelékek

1. sz. melléklet Archiválási osztály elemzési tábla

Archiválási_Osztály_Elemzés_v.1.0.xlsx

2. sz. melléklet Archiválási osztály összesítő tábla

Archiválási_Osztály_Összesítő_v1.0.xlsx

3. sz. melléklet Futárjegyzék és NISZ értesítés beküldött adatállományról

NISZ-nek küldendő jegyzőkönyv, futárjegyzék elérhetősége: http://www.police.hu/futar,
NISZ-nek küldendő jegyzőkönyv.xlsx

Dr. Kőszegi Károly 0192 1. Tatabánya Önálló Bírósági Végrehajtó

[redacted]