VESZPRÉMI
TANKERÜLETI
KÖZPONT

A Veszprémi Tankerületi Központ 2/2023. (XI . 02 .) számú Archiválási szabályzata

Kiadta:

Veszprém, 2023. 11 02.

Veszprémi Tankerületi Központ 01

.....

Szauer István
tankerületi igazgató
Veszprémi Tankerületi Központ

A Veszprémi Tankerületi Központ jelen Szabályzatát az állami köznevelési közfeladat ellátásában fenntartóként részt vevő szervekről, valamint a Klebelsberg Központról szóló 134/2016. (VI. 10.) Korm. rendelet 5. § (2) bekezdés 9. pontjában biztosított középirányítói hatáskörömben eljárva, a Klebelsberg Központ Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás 1. mellékletének 40. §-a alapján jóváhagyom:

Budapest, 2023. November „16."

Klebelsberg Központ Elnök

.....

Hajnal Gabriella
elnök
Klebelsberg Központ

DOKUMENTUM KONTROLL

Szabályzat alapadatai

Szabályzatot kiadó szerv megnevezése	**Veszprémi Tankerületi Központ**
Szabályzat egységes/egyedi jellegének megjelölése	**Egyedi**
Archiválási szabályzat szervi hatálya (egységes szabályzat esetén a szabályzat hatálya alá tartozó szervek felsorolása)	**Veszprémi Tankerületi Központ**

Változások

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
v1.0	2023.11.02	Szabályozási környezet kialakítása

Szabályozás elkészítéséért felelős

Verzió	Elfogadás dátuma	Beosztás	Név
v1.0	2023.11.02	Veszprémi Tankerületi Központ, Gazdálkodási, Üzemeltetési és Pályázati Főosztály	Porkoláb Péter

Szakmai tartalomért felelős szakterület

Verzió	Elfogadás dátuma	Beosztás	Név
v1.0	2023.11.02	Veszprémi Tankerületi Központ, Gazdálkodási, Üzemeltetési és Pályázati Főosztály	Porkoláb Péter

Nyilvántartás

Dokumentum kiadásáért és nyilvántartásért felelős	**Dr. Gulyás Edina**

Kiadás

Készült	2 eredeti példányban
Kapják	1 eredeti példány: Veszprémi Tankerületi Központ 1 eredeti példány: Klebelsberg Központ Elektronikusan: Elektronikus Ügyintézési Felügyelet (DMÜ)

Tartalomjegyzék

DOKUMENTUM KONTROLL **2**
I. FEJEZET **4**
ÁLTALÁNOS RENDELKEZÉSEK 4
1. A Szabályzat célja 4
2. A Szabályzat személyi hatálya 4
3. A Szabályzat tárgyi hatálya 4
4. A Szabályzat alkalmazási területe 4
5. A Szabályzat során alkalmazandó jogszabályok köre 5
6. Értelmező rendelkezések 5
II. FEJEZET **6**
RÉSZLETES RENDELKEZÉSEK 6
7. Az archiválási folyamat résztvevői 6
8. Kockázatelemzés 7
9. Az archiválás folyamata 9
10. Archiválás dokumentálása 10
11. A tárolt és mentésre kerülő adatok köre 10
12. Tesztelés 10
13. Az adattrezor-archiválás ellenőrzése 10
III. FEJEZET **10**
ZÁRÓ RENDELKEZÉSEK 10
1. számú melléklet – A PSZD archiválási osztály elemzési tábla 11
2. számú melléklet – Archiválási osztályba sorolás összesítő tábla 12

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény, 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 előírásainak figyelembevételével, a Veszprémi Tankerületi Központ Szervezeti és Működési Szabályzatának 5. § (2) bekezdés f) és g) pontjában biztosított jogkörömben eljárva a Veszprémi Tankerületi Központ informatikai rendszereinek és információvagyonának mentésére, archiválására vonatkozó feladatokat, kötelezettségeket az alábbiak szerint szabályozom.

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja

1. § (1) A Szabályzat célja, hogy meghatározza a Veszprémi Tankerületi Központ (a továbbiakban: Tankerületi Központ) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) 25. § (4a) bekezdése szerinti, az ügyek intézésével kapcsolatos elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentésével és adattrezor szolgáltatást nyújtó őrző szervhez továbbításával, valamint a kapcsolódó folyamatokkal kapcsolatos részletszabályokat.

(2) Az adattrezor-archiválási kötelezettség célja a Tankerületi Központnak az e-ügyintézési kötelezettség teljesítésével összefüggő adatok sérüléséből eredő működési zavara esetén a működési képesség helyreállítása és az adatvesztés minimalizálása.

2. A Szabályzat személyi hatálya

2. § A Szabályzat hatálya kiterjed a Tankerületi Központra, mint adatkezelőre, a Tankerületi Központ belső információs rendszereit üzemeltető szervezeti egységeire, a Tankerületi Központ igazgatójára, gazdasági vezetőjére, szakmai vezetőjére, kormányzati szolgálati jogviszonyban foglalkoztatott alkalmazottjaira, munkavállalóira, munkavégzésre irányuló egyéb jogviszony alapján a Tankerületi Központ által foglalkoztatott személyekre, valamint az üzemeltetésben, a Tankerületi Központ általi mentési archiválási folyamatban résztvevő, illetve azt szerződés alapján végző harmadik személyekre.

3. A Szabályzat tárgyi hatálya

3. § A Szabályzat tárgyi hatálya az elektronikus ügyintézés részét képező vagy ahhoz szervesen kapcsolódó minden, a Tankerületi Központ által üzemeltetett informatikai rendszerre (hardver, operációs rendszer, alkalmazás szerver, alkalmazás, adatbázis szerver, adatbázis, web szerver, file szerver, dokumentum kezelő) kiterjed, így különösen a Tankerületi Központ által használt KRÉTA – POSZEIDON Irat és Dokumentumkezelő rendszerre (a továbbiakban: POSZEIDON rendszer).

4. A Szabályzat alkalmazási területe

4. § A Szabályzat rendelkezéseit az elektronikus ügyintézés részét képező vagy ahhoz szervesen kapcsolódó minden informatikai rendszer esetében a Szabályzatban részletezett módon teljes-körűen alkalmazni kell.

5. § (1) Az adattrezor-archiválási kötelezettség a Tankerületi Központot, mint elektronikus ügyintézést biztosító szervet terheli az általa saját szoftverkörnyezetben kezelt elektronikus információs rendszereiben és a nyilvántartásaiban tárolt nem minősített adatok tekintetében, vagy azokkal együtt a teljes futtatási környezet tekintetében.

(2) A Tankerületi Központ Hivatali Kapu rendszerei a POSZEIDON rendszerbe be vannak kötve, ezért a Hivatali Kapun keresztül érkező és az onnan kiküldött küldemények archiválási és trezorálási feladatait a Klebelsberg Központ által megbízott adatfeldolgozók végzik. Így biztosított, hogy az

archivált adatokból az eredeti környezet teljes vagy részleges megsemmisülése esetén helyreállítható legyen az eredeti működés a megfelelő hardvereszközök üzembe helyezését követően.

(3) Az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet szerint a Tankerületi Központ az elektronikus ügyintézés biztosításához szükséges elektronikus információs rendszerei az *1. számú mellékletben* jelölt archiválási osztályba tartoznak, melyek archiválását az ott meghatározott gyakorisággal a Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság (a továbbiakban: NISZ Zrt.) és az Educational Development Informatikai Vagyonkezelő Zártkörűen Működő Részvénytársaság (a továbbiakban: EDUDEV Zrt.) együttműködésében a Klebelsberg Központtal kötött üzemeltetési szerződés alapján kell elvégezni. A Tankerületi Központ elektronikus információs rendszerei archiválási osztályba sorolását összesítő táblázat a *2. számú mellékletben* található.

5. A Szabályzat során alkalmazandó jogszabályok köre

6. § A Szabályzat alkalmazása során figyelemmel kell lenni különösen az alábbi jogszabályok rendelkezéseire:

a) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (E-ügyintézési tv.),

b) az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet,

c) az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról szóló 466/2017. (XII. 28.) Korm. rendelet,

d) a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet (a továbbiakban: NFM rendelet),

e) a belföldi Állami Futárszolgálat tevékenységének szabályozásáról szóló 44/1998. (X. 14.) BM rendelet (a továbbiakban: BM rendelet).

6. Értelmező rendelkezések

7. § A Szabályzat értelmében:

1. *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,

2. *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. A Szabályzatban adatfeldolgozó szerv alatt a NISZ Zrt.-t és az EDUDEV Zrt.-t értjük,

3. *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,

4. *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,

5. *adattrezor-archiválás:* az E-ügyintézési törvény 25. § (4a) bekezdése szerinti, az elektronikus ügyintézést biztosító szervnek az ügyek intézésével kapcsolatos, elektronikus információs

rendszereiben és nyilvántartásaiban tárolt nem minősített adatai mentése, mely nem azonos az adatok az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerinti biztonsági mentésével,

6. *archiválás:* a nem, vagy nagyon ritkán használt, de megőrzendő adatok áthelyezése a feldolgozó rendszer tárolójáról egy másik, elkülönített tárolóra,
7. *BCP (business continuity planning):* működés folytonossági terv,
8. *DRP (data recovery planning):* adat helyreállítási terv,
9. *elektronikus információs rendszer (EIR):* az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók) és szoftverek együttese,
10. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye,
11. *kockázatelemzés*: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése,
12. *kormányzati adattrezor (KAT):* olyan kormányzati adatbank, amely az adattrezor-archivált állományokat fogadja és biztonságosan tárolja, őrzi, és az adatok adatkezelő részére történő kiadásával újraépíthetővé teszi a különböző informatikai rendszereket,
13. *őrzésért felelős szerv:* a NISZ Zrt.,
14. *rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek,
15. *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,
16. *teljes (full) mentés:* minden kiválasztott elem mentésre kerül,
17. *teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem,
18. *visszaállítás:* meghibásodás vagy sérülés miatt leállt informatikai szolgáltatás helyreállítása, amely megkívánhatja a rendszerek és adatbázisok mentéseinek visszatöltését. Katasztrófaelhárítás esetén leginkább a gyors, ideiglenes szolgáltatás visszaállítást jelenti, megkülönböztetve a végleges helyreállítástól,
19. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem,

II. FEJEZET

RÉSZLETES RENDELKEZÉSEK

7. Az archiválási folyamat résztvevői

8. § (1) A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Tankerületi Központ ügyintézési ciklusával.

(2) Az 5. § (2) bekezdésével összefüggően a Tankerületi Központ által használt Hivatali Kapuk archiválási folyamatát a Klebelsberg Központ megbízásából a NISZ Zrt. és az EDUDEV Zrt. végzi.

(3) Az 5. § (2) bekezdés szerinti esetben az archiválási folyamat során keletkező adatállományok kézbesítésére vonatkozó feladatokat a belföldi Állami Futárszolgálat látja el BM rendeletben foglaltaknak megfelelően.

8. Kockázatelemzés

9. § (1) A Tankerületi Központ informatikai szolgáltatásainak helyreállítási terveit, valamint a fontos informatikai szolgáltatások meghatározásához szükséges kockázatelemzést a Klebelsberg Központ megbízása alapján a NISZ Zrt. végzi.

(2) Az informatikai rendszerek megbízható működése és az ügymenet folytonossága a NISZ Zrt. feladata. Az alábbiakban részletezett eszközök, rendszerek szolgáltatások meghibásodása esetén a Tankerületi Központnak haladéktalanul bejelentési kötelezettsége van először a NISZ Zrt., majd azt követően a Klebelsberg Központ Informatikai Főosztálya felé.

(3) Az elvárt működési biztonság a következőkben ismertetett szabályok és módszerek alkalmazásán keresztül érhető el, melyek a NISZ Zrt. közreműködésével valósulnak meg:

a) el kell készíteni a fontos informatikai szolgáltatások helyreállítási terveit,

b) a fontos informatikai szolgáltatások meghatározásához kockázatelemzést kell végezni,

c) az azonosított szolgáltatásoknál meg kell vizsgálni a kulcsfontosságú elemeket, így:

   ca) meg kell határozni a még tolerálható helyreállítási időket,

   cb) el kell készíteni a helyreállítási terveket és azokat a gyakorlatban is tesztelni kell.

d) főszabályként a következőt kell alkalmazni a kockázatok megosztásánál: a szoftverkörnyezet infrastrukturális hibája esetén – ideértve a hálózatot, hálózati tárolót, internetkapcsolatot, virtualizációt – az elsődleges felelős az NFM rendelet szerinti központi szolgáltató, mely alatt jelen szabályzatban a NISZ Zrt.-t értjük. A NISZ Zrt., valamint a Klebelsberg Központ Informatikai Főosztálya felé a Tankerületi Központnak csak hibabejelentési kötelezettsége áll fenn.

(4) Az alkalmazáskörnyezet meghibásodása esetén – ideértve a külső támadást, szoftver termék hibát, az elsődleges felelősség a NISZ Zrt. terheli, míg az emberi mulasztásból eredő hibák esetén a Tankerületi Központot terheli.

10. § (1) A működésfolytonosság (BCP) és DRP kockázatkezelés a 9. §-ban foglaltak figyelembevételével, a NISZ Zrt. közreműködésével történik.

(2) Az informatikai rendszer és az eszközeinek időszakos leállásából, kieséséből, működési zavaraiból adódó lehetséges kockázatok típusai a működésfolytonossággal (BCP) összefüggésben, azok hatása, valamint azok kezelése és helyreállítása a (3) - (5) bekezdésben kerülnek meghatározásra. Az NFM rendelet 2. §-a szerint a központosított informatikai szolgáltatásokat a Tankerületi Központ a NISZ Zrt.-től a Klebelsberg Központon keresztül veszi igénybe. A Klebelsberg Központ és a NISZ Zrt. között érvényben lévő egyedi szolgáltatási megállapodás alapján az egyes szolgáltatások helyreállítási ideje tekintetében a NISZ Zrt. szolgáltatáskatalógusában SLA01 szolgáltatási szinten rögzített időtartamok érvényesek, a (3)-(5) bekezdésekben feltüntetettek szerint.

(3) A működésfolytonosság (BCP) és az internet kapcsolat (WAN World Area Network) kiesésének összefüggései:

a) hatása az ügymenetre: kritikus (valamennyi felhőalapú rendszer elérhetetlenné válik),

b) valószínűsége: magas rendelkezésre állás miatt évente legfeljebb 1 alkalom,

c) helyreállítása idő: a bejelentések 90%-ában legfeljebb 12 munkaóra,

d) kockázatkezelés:

   da) az esetet a NISZ Zrt. és a Klebelsberg Központ Informatikai Főosztálya felé is be kell jelenteni,

   db) a szolgáltatás minősége és a szolgáltatási szint (SLA) a NISZ Zrt. és a Klebelsberg Központ közötti szerződésben definiáltak alapján értendők,

e) helyreállítás (DRP):

ea) fővonal hiba esetén: hibabehatárolás, a hiba jelentése a NISZ Zrt.-nek, az érintettek tájékoztatása - ideértve a Klebelsberg Központ Informatikai Főosztályát -, az incidens és az elhárítás dokumentálása,

eb) router/modem hiba esetén: hibabehatárolás, a hiba jelentése a NISZ Zrt.-nek, az érintettek tájékoztatása - ideértve a Klebelsberg Központ Informatikai Főosztályát -, funkcionális csereeszköz haladéktalan igénylése a NISZ Zrt.-től, tesztelés, próbaüzem, éles üzem.

(4) A működésfolytonosság (BCP) és a belső hálózat (LAN Local Area Network) elemeinek meghibásodásával kapcsolatos összefüggések:

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

b) valószínűsége évente legfeljebb egyszer,

c) helyreállítási idő: a bejelentések 90%-ában legfeljebb 12 munkaóra,

d) 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, amelyek a Szolgáltató feladatát képezik,

e) helyreállítás (DRP):

ea) aktív elem meghibásodása esetén: hibabehatárolás, a hiba jelentése a NISZ Zrt.-nek, az érintettek - ideértve a Klebelsberg Központ Informatikai Főosztályát - tájékoztatása, funkcionális csereeszköz beállítása és konfigurálása, tesztelés, próbaüzem, éles üzem, dokumentálás,

eb) passzív elem (kábel, rack, stb.) meghibásodása esetén: hibabehatárolás, a hiba jelentése a NISZ Zrt.-nek, az érintettek - ideértve a Klebelsberg Központ Informatikai Főosztályát - tájékoztatása, a passzív szakasz, vagy alkatrész cseréje, tesztelés, próbaüzem, éles üzem, dokumentálás.

(5) A működésfolytonosság (BCP) és a hálózati tároló (SAN) meghibásodásával kapcsolatos összefüggések:

a) hatása az ügymenetre: lényeges (minden szerveren tárolt dokumentum és onnan futó szolgáltatás elérhetetlenné válhat),

b) valószínűsége: háromévente egyszer,

c) helyreállítási idő: a bejelentések 90%-ában legfeljebb 13 munkaóra,

d) kockázatkezelés:

da) az esetet NISZ Zrt.-nek, illetve a Klebelsberg Központ Informatikai Főosztályának is be kell jelenteni,

db) a szerződésben törekedni kell arra, hogy az SLA (Service Level Agreement) alapú legyen, azaz a szolgáltatás minőségétől függ a szolgáltatási díj, és 99,95%-os rendelkezésre állást biztosítson.

e) helyreállítás (DRP):

ea) fővonal hiba esetén: hibabehatárolás, a hiba jelentése, az érintettek tájékoztatása – ideértve a Klebelsberg Központ Informatikai Főosztályát –, az eset a NISZ Zrt.-nél történő haladéktalan bejelentése, az incidens és az elhárítás dokumentálása,

eb) router/modem hiba esetén: hibabehatárolás, a hiba jelentése, az érintettek tájékoztatása – ideértve a Klebelsberg Központ Informatikai Főosztályát –,

funkcionális csereeszköz haladéktalan igénylése a Szolgáltatótól, tesztelés, próbaüzem, éles üzem.

9. Az archiválás folyamata

11. § (1) A mentési, archiválási rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell annak érdekében, hogy minimalizálni lehessen az emberi tényezőből adódó hibák előfordulásának valószínűségét.

(2) A mentéseknek ki kell terjednie a működési folyamatok és tevékenységek támogatásában és kiszolgálásában részt vevő informatikai eszközökre, illetve azok elhelyezésére szolgáló kiszolgáló rendszerekre/infrastruktúrákra.

(3) A NISZ Zrt. és az EDUDEV Zrt. közös felelőssége a Klebelsberg Központtal kötött szolgáltatási szerződés alapján, hogy a jelen Szabályzatban foglalt gyakorisággal gondoskodjon az érintett EIR rendszerek mentéséről, a mentések tárolása fizikailag biztonságos legyen. Védeni kell őket az illetéktelen hozzáférésektől, illetve a különböző fizikai behatásoktól (tűz, víz, mágnesesség, stb.).

(4) 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 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, stb.).

(5) A rendszer működésének fenntartása céljából, első alkalommal, valamint minden teljes állomány mentése esetén valamennyi elektronikus információs rendszer vagy nyilvántartás esetében az összes adatot, azzal együtt a teljes futtatási környezetet és a rendszer teljes dokumentációját archiválni kell. A dokumentációnak tartalmaznia kell a rendszer sikeres telepítéséhez, üzemeltetéséhez, a felhasználói oktatáshoz, a rendszer továbbfejlesztéséhez szükséges – a szervezet rendelkezésére álló – összes információt, valamint az állam tulajdonában lévő forráskódot is. A dokumentációnak alkalmasnak kell lennie arra, hogy a benne foglaltak alapján a rendszer megsemmisülése esetén az elektronikus információs rendszer személyfüggetlen módon lépésenként visszaállítható legyen. A változások archiválása a legutóbbi teljes mentéshez képest úgy történik, hogy a legutolsó adat- és dokumentációállomány, továbbá a futtatási környezet helyreállítható legyen.

(6) Az adattrezor-archiválást titkosító kulcs alkalmazásával az adatfeldolgozó úgy végzi, hogy abból az adatkezelőnél működtetett elektronikus információs rendszerek visszaállíthatóak legyenek. Az adatfeldolgozónak jól beazonosítható módon meg kell jelölnie, hogy az átadott adatállomány mely adatkezelő elektronikus információs rendszer archiválását tartalmazza. Az adattrezor-archiválásnak tartalmaznia kell a visszaállításhoz szükséges dokumentációt.

(7) Az őrzésért felelős szervnek átadásra kerülő adatállománynak a technika archiváláskori állása szerint rosszindulatú szoftverkódtól való mentessége az adatfeldolgozó felelőssége.

12. § Az archiválási folyamat főbb szakaszai:

a) az üzemeltető (jelen Szabályzatban üzemeltető alatt a POSZEIDON rendszer üzemeltetőjét értjük) végzi az érintett adatállomány kijelölését és mentését az adatmennyiségtől függő típusú tartós adathordozóra, illetve annak ellenőrzését,

b) az üzemeltető végzi a mentett adatokat tartalmazó adathordozó titkosítását,

c) az adathordozó átvételét és a KAT-ba szállítását a NISZ Zrt. megrendelése alapján az Állami Futárszolgálat végzi.

10. Archiválás dokumentálása

13. § (1) Az archiválás naplózása gépi alapú. A titkosított mentési állomány mellé egy titkosítatlan szöveg fájlt kell elkészíteni, amely a mentett állományok felsorolását tartalmazza.

(2) Az (1) bekezdésben megjelölt szöveg fájl megőrzési ideje megegyezik a vonatkozó mentési állomány megőrzési idejével.

(3) A mentési média típusa: elektronikus adathordozó.

11. A tárolt és mentésre kerülő adatok köre

14. § A POSZEIDON rendszer a Hivatali Kapu szerverein keresztül érkezett és onnan küldött küldemények automatikus letöltésére, illetve a manuálisan iktatott küldemények elektronikus iktatására és az elektronikusan tárolt dokumentumok nyilvántartására szolgál.

12. Tesztelés

15. § (1) 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.

(2) A Klebelsberg Központ és a biztonsági mentést végző NISZ Zrt és az EDUDEV Zrt. között fennálló szolgáltatási szerződések alapján a Klebelsberg Központ beszámoltatja a NISZ Zrt.-t és az EDUDEV Zrt.-t a biztonsági mentésről arra vonatkozóan, hogy hitelt érdemlően igazolja az archivált és mentett adatállományból az eredeti állapot helyreállíthatóságát a biztonsági mentési állományok, ill. archivált állományok alapján. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

13. Az adattrezor-archiválás ellenőrzése

16. § (1) Az archiválás ellenőrzésére az Elektronikus Ügyintézési Felügyelet jogosult.

(2) A Felügyelet az adattrezor-archiválási kötelezettség végrehajtását az adatkezelőnél ellenőrzi. Ennek keretében az adattrezor-archiválásból – előzetes bejelentési kötelezettség mellett – próba-visszaállítást rendelhet el. A próba-visszaállítás végrehajtásakor figyelemmel kell lenni arra, hogy az ne eredményezzen aránytalan mértékű szolgáltatáskiesést, valamint ne veszélyeztesse az érintett elektronikus információs rendszer működését. A próba-visszaállítás sikeres, ha a szervezet működésében zavar nem keletkezik, és az adattrezor-archiválásban foglalt valamennyi adat hiánytalanul és hibamentesen visszaállításra kerül.

III. FEJEZET

ZÁRÓ RENDELKEZÉSEK

17. § (1) A Szabályzat a Klebelsberg Központ elnökének jóváhagyását követő napon lép hatályba.

(2) A Szabályzatot évente, vagy jelentősebb infrastrukturális változás, illetve jogszabályváltozás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell.

(3) A Szabályzat módosítása esetén a módosított szabályzatot az Elektronikus Ügyintézési Felügyelet részére felülvizsgálatra meg kell küldeni.

1. számú melléklet – A PSZD archiválási osztály elemzési tábla

Az EIR-hez tartozó alapadatok 3.0	
Az Elektronikus Információs Rendszer neve:	KRÉTA – POSZEIDON Irat és Dokumentumkezelő rendszer
EIR rövid kódja:	PSZD
EIR állapota:	folyamatban
Adatkezelő szervezet megnevezése:	Veszprémi Tankerületi Központ
Adatfeldolgozó szervezet megnevezése:	NISZ Zrt. és EDUDEV Zrt.
Mentési osztályba sorolás dátuma:	Szabályzat kiadásának dátuma
EÜF kapcsolattartó megnevezése	Tankerületi Központ által kijelölt személy
EÜF kapcsolattartó elérhetősége (e-mail, telefon)	Tankerületi Központ hivatali elérhetősége
Egy teljes mentés mérete (Mbyte-ban)	nem meghatározható, változó
Az EIR rövid leírása:	A KRÉTA – POSZEIDON Irat és Dokumentumkezelő rendszerbe integrált Hivatali Kapuk (HKP) a Központi Elektronikus Szolgáltató Rendszer (központi rendszer, KR) részei. A HKP-n keresztül az igénybe vevő szervezetek hitelesen tudnak fogadni elektronikus üzeneteket, illetve a hivatalok elektronikus üzenetei a hitelesen azonosított ügyfelekhez (állampolgár, hivatal, gazdálkodó szervezet) eljuttathatók a KRÉTA – POSZEIDON Irat és Dokumentumkezelő rendszeren keresztül iktatott, dokumentált formában.
Archiválási kategória meghatározása (nem kitölthető)	
Az EIR archiválási osztálya	**3. kategória**
AZ EIR archiválásának módja	>Első alkalommal, valamint legalább felévente teljes állomány archiválása >Havonta változások archiválása > Kisméretű archív állomány (300 MB alatt) esetén, minden esetben teljes állomány archiválása szükséges > A hatósági ellenőrzés éves ellenőrzési terv szerint

2. számú melléklet – Archiválási osztályba sorolás összesítő tábla

	Archiválási osztályba sorolás összesítő táblázat						
	Adatkezelő szervezet megnevezése:	Veszprémi Tankerületi Központ					
Sorsz.	**Az Elektronikus Információs Rendszer neve**	**EIR rövid kódja**	**EIR állapota**	**Adatfeldolgozó szervezet megnevezése**	**Mentési osztályba sorolás dátuma**	**EÜF kapcsolattartó megnevezése**	**EÜF kapcsolattartó elérhetősége (e-mail, telefon)**
1	KRÉTA – POSZEIDON Irat és Dokumentumkezelő rendszer	PSZD	Folyamatban	NISZ Zrt. és EDUDEV Zrt.	Szabályzat kiadásának dátuma	Informatikai kapcsolattartó	Tankerületi Központ hivatali elérhetősége