




SZIGETVÁRI TANKERÜLETI KÖZPONT


Iktatószám: TK/020/00335-5/2022

A Szigetvári Tankerületi Központ 5/2022. (XII. 15) számú Archiválási szabályzata

Kiadta:

Szigetvár, 2022. december 15.


Bogár László
tankerületi igazgató
Szigetvári Tankerületi Központ



A Szigetvári Tankerületi Központ jelen Szabályzatát az állami köznevelési közfeladat ellátásában fenntartóként részt vevő szervekről, valamint a Klebelsberg Központtról 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, 2022. december 21.


Hajnal Gabriella
elnök
Klebelsberg Központ



Tartalomjegyzék

I. FEJEZET.....	4
ÁLTALÁNOS RENDELKEZÉSEK.....	4
1. A szabályzat célja	4
2. A szabályzat során alkalmazandó jogszabályok köre	4
3. Értelmező rendelkezések	4
4. A Tankerületi Központ által ellátandó tevékenységek köre.....	7
5. A szabályzat alkalmazása	7
6. A szabályzat személyi hatálya.....	7
7. A szabályzat tárgyi hatálya	8
8. Kapcsolódó szabályzatok, eljárások, rendelkezések.....	8
II. FEJEZET	8
KÜLÖNÖS RENDELKEZÉSEK	8
9. Az archiválási folyamat résztvevői	8
10. Kockázatelemzés	9
11. Az archiválás folyamata	11
12. A tárolt és mentésre kerülő adatok köre	11
13. Hatósági ellenőrzés	11
14. Tesztelés	12
III. FEJEZET.....	12
ZÁRÓ RENDELKEZÉSEK	12
1. számú melléklet: Archiválási osztályba sorolás összesítő táblázat	13
2. számú melléklet: A PSZDN archiválási osztály elemzési táblája	14

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 ügyintézással összefüggő adatok biztonságát szolgáló Kormányzati Adattrezzorról szóló 466/2017. (XII. 28.) Korm. rendelet előírásainak figyelembevételével, a Szigetvári Tankerületi Központ Szervezeti és Működési Szabályzatának 5. § (2) bekezdés f) pontjában biztosított jogkörömben eljárva a Szigetvári 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 Szigetvári 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, és a kapcsolódó folyamatokkal kapcsolatos részletszabályokat.

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

2. A szabályzat során alkalmazandó jogszabályok köre

2. § A szabályzat alkalmazása során figyelemmel kell lenni különösen az alábbi jogszabályok rendelkezéseire:

- a) E-ügyintézési tv.,
- b) az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet,
- c) az elektronikus ügyintézással összefüggő adatok biztonságát szolgáló Kormányzati Adattrezzorról szóló 466/2017. (XII. 28.) Korm. rendelet (a továbbiakban: 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).

3. Értelmező rendelkezések

3. § E 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. Jelen szabályzatban adatfeldolgozó szerv alatt a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaságot értjük.

3. *adatgazda*: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik,
4. *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,
5. *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 végrehajttatja,
6. *archiválás*: a nem, vagy nagyon ritkán használt, de megőrzendő adatok áthelyezése a feldolgozó rendszer tárolójáról egy másik, elkülönített tárolóra,
7. *archiválási eljárás*: az archiválási stratégiát végrehajtó informatikai folyamat,
8. *archiválási szolgáltatás*: az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás,
9. *archiválási politika*: az archiválandó tartalomra vonatkozó szakmai elvárások, valamint az archivált adatok eléréséhez kapcsolódó szakmai követelmények meghatározása,
10. *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,
11. *automatikus információátadás*: információátadás az információ átadását biztosító együttműködő szerv részéről emberi beavatkozást nem igénylő módon,
12. *automatikus információátadási felület*: az információ átadását biztosító együttműködő szerv által létrehozott és üzemeltetett, automatikus információátadást lehetővé tevő műszaki megoldás,
13. *BCP (business continuity planning)*: működés folytonossági terv,
14. *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,
15. *DRP (data recovery planning)*: adat helyreállítási terv,
16. *elektronikus információs rendszer (EIR)*: 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,
17. *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,

18. *folytonos védelem*: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem,
19. *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.
20. *kockázat*: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye,
21. *kockázatokkal arányos védelem*: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével,
22. *központi mentés*: alapértelmezésben a mentések a rendszerbe állított központi mentőeszköz igénybevételével történnek,
23. *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,
24. *kritikus szolgáltatás*: informatikai szolgáltatás, amely a szervezet működése szempontjából létfontosságú,
25. *offline mentés*: a mentés a szolgáltatások leállításával történik, a szolgáltatások a mentés ideje alatt nem érhetőek el,
26. *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,
27. *őrzésért felelős szerv*: a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság,
28. *rendelkezésre állás*: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek,
29. *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,
30. *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,
31. *teljes (full) mentés*: minden kiválasztott elem mentésre kerül,
32. *teljes körű védelem*: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem,

33. *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,
34. *zárt védelem*: az összes számításba vehető fenyegetést figyelembe vevő védelem.

4. A Tankerületi Központ által ellátandó tevékenységek köre

4. § (1) Az adattrezor-archiválási kötelezettség a Tankerületi Központot, mint elektronikus ügyintézőt biztosító szervezet 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 szerverein keresztül érkező és onnan kiküldött küldemények archiválási és trezorálási feladatait a Klebelsberg Központ által megbízott adatfeldolgozó végzi, biztosítva, hogy az archivált adatokból az eredeti környezet teljes vagy részleges megsemmisítése esetén helyreállítható legyen az eredeti működés a megfelelő hardvereszközök üzembe helyezését követően.

(3) A Tankerületi Központnak az elektronikus ügyintézés biztosításához szükséges elektronikus információs rendszereit a Korm. rendelet szerint archiválási osztályba kell besorolnia, archiválásukat az ott meghatározott gyakorisággal kell elvégeznie. A Tankerületi Központ archiválási osztályba sorolás összesítő táblázatát ld. az *1. számú mellékletben*, az archiválási kategória meghatározását ld. a *2. számú mellékletben*.

(4) A rendszer működésének fenntartása céljából, első alkalommal valamennyi elektronikus információs rendszer vagy nyilvántartás esetében az összes adatot, azzal együtt a teljes futtatási környezetet és a rendszer teljes dokumentációját archiválni kell. A változások archiválása a legutóbbi teljes mentéshez képest történik úgy, hogy a legutolsó adat- és dokumentációállomány, továbbá a futtatási környezet helyreállítható legyen.

(5) Az adattrezor-archiválást titkosító kulcs alkalmazásával az adatfeldolgozó úgy végzi, hogy abból az adatkezelőnél működtetett elektronikus információs rendszerek külön-külön is 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.

(6) Az őrzésért felelős szervnek átadásra kerülő adatállománynak a technika archiváláskori állása szerint rosszindulatú szoftverködtől való mentessége a Tankerületi Központ felelőssége.

5. A szabályzat alkalmazása

5. § Jelen szabályzat rendelkezéseit az elektronikus ügyintézés részét képező vagy ahhoz szervesen kapcsolódó minden informatikai rendszer esetében a jelen szabályzatban részletezett módon teljes körűen alkalmazni kell.

6. A szabályzat személyi hatálya

6. § 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 mentési archiválási folyamatban résztvevő, illetve azt szerződés alapján végző harmadik személyekre.

7. A szabályzat tárgyi hatálya

7. § 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) terjed ki:

- a) Hivatali Kapu szerverei (HKP):
 - aa) Szigetvári Tankerületi Központ (SZIGTANKER, KRID: 651169363) (általános ügyek),
 - ab) Szigetvári Tankerületi Központ HR, Köznevelési és Humánpolitikai Főosztály (SZTKHR, KRID: 168445718) (általános munkaügyek),
 - ac) Szigetvári Tankerületi Központ IVK, Köznevelési és Humánpolitikai Főosztály (SZTKIVK, KRID: 666495104) (intézményvezető kinevezések).
- b) KRÉTA - Poszeidon Irat és Dokumentumkezelő rendszer.

8. Kapcsolódó szabályzatok, eljárások, rendelkezések

8. § Jelen szabályzat alkalmazása során figyelemmel kell lenni különösen a Tankerületi Központ alábbi szabályzatainak rendelkezéseire:

- a) a Tankerületi Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzata, 2017
- b) a Tankerületi Központ panaszokkal és közérdekű bejelentésekkel kapcsolatos eljárásról szóló szabályzata ,
- c) a Tankerületi Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzata.

II. FEJEZET

KÜLÖNÖS RENDELKEZÉSEK

9. Az archiválási folyamat résztvevői

9. § (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 adatfeldolgozó feladata az adattrezor-archiválással kapcsolatos rendszeres és időszakos biztonsági mentések elvégzése. Az *1. sz. mellékletben* meghatározott információs rendszernél, ahol a Tankerületi Központ a Klebelsberg Központ közreműködésével adatfeldolgozóként, adattovábbítóként a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaságot (a továbbiakban: NISZ Zrt.) veszi igénybe, a mentés az adatfeldolgozó, adattovábbító közreműködésével történik, az adatbázisok konzisztenciájának biztosításával és az egyéb munkaállomások hálózati munkájának akadályozása nélkül.

(3) Az elektronikusan kezelt ügyekre vonatkozóan, amelyeket a Tankerületi Központ a Hivatali Kapu szerverein a KRÉTA - Poszeidon Irat és Dokumentumkezelő rendszerben kezel, a jelen szabályzatban meghatározottak az irányadók.

10. Kockázatelemzés

10. § (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, emberi mulasztást – az elsődleges felelősség a Tankerületi Központot terheli.

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

(2) Az informatikai rendszer és az eszközeinek időszakos leállításából, kieséséből, működési zavarából 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 elérhetlenné válik),
- b) valószínűsége: magas rendelkezésre állás miatt évente legfeljebb 1 alkalom,
- c) helyreállítási 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 hálózathoz),
- 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.

11. Az archiválás folyamata

12. § (1) A mentési, archiválási rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőtől 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. felelőssége a Klebelsberg Központtal között szolgáltatási szerződés alapján, hogy 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 információvagyon 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).

(5) A Tankerületi Központ információs rendszerei – a jelen szabályzat mellékletei szerint 3-as kategóriákba kerültek besorolásba. A 3-as kategóriába sorolt rendszerekről első alkalommal, valamint fél évente teljes adatállomány archiválás történik, továbbá archiválás történik havonta a változásokról.

(6) A jelen §-ban foglalt feladatokat a hatályban lévő jogszabályi kijelölések, valamint a Klebelsberg Központtal fennálló szolgáltatási szerződés alapján a NISZ Zrt. végzi.

13. § 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.

12. A tárolt és mentésre kerülő adatok köre

14. § (1) A tárolt és mentésre kerülő adatok köre:

Az Elektronikus Információs Rendszer neve	EIR rövid kódja	EIR állapota
KRÉTA - Poszeidon Irat és Dokumentumkezelő rendszer	PSZDN	Folyamatban

(2) A KRÉTA - Poszeidon Irat és Dokumentumkezelő rendszer a Hivatali Kapu szerverein keresztül érkezett küldemények automatikus letöltésére, illetve a manuálisan iktatott küldemények elektronikus iktatására és az elektronikusan tárolt dokumentumok nyilvántartására szolgál.

13. Hatósági ellenőrzés

15 § (1) A jelen szabályzatban meghatározott információs rendszerek archiválása az osztályba sorolást követően az előírt gyakorisággal történik.

(2) Az archiválások gyakoriságának összhangban kell állnia a mentett adatok, illetve programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Tankerületi Központ ügyintézési ciklusával.

14. Tesztelés

16. § A biztonsági mentéseket hibajelzés-mentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szűrőpróbaszerűen tesztelni kell, illetve automatikus ellenőrzéseket kell végrehajtani. A Tankerületi Központ felelőssége a biztonsági mentést végző NISZ Zrt. beszámoltatása 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.

II. FEJEZET

ZÁRÓ RENDELKEZÉSEK

17. § (1) A szabályzat a kiadmányozását követő napon lép hatályba.

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

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

1. számú melléklet: Archiválási osztályba sorolás összesítő táblázat

Sorsz.	Az elektronikus Információs rendszer neve	EIR Kódja	EIR Állapota	Adatgazda neve	Adatgazda Elérhetősége (e-mail, telefon)	Adatfeldolgozó szervezet megnevezése	Mentési osztályba sorolás dátuma	EÜF kapcsolattartó megnevezése	EÜF kapcsolattartó elérhetősége (e-mail, telefon)
1	KRÉTA - Poszeidon Irat és Dokumentumkezelő Rendszer	PSZDN	Folyamatban	Igazgató (Szigetvári Tankerületi Központ)	központi email és telefon	NISZ Zrt.	2022.12.31	információbiztonsági felelős	szigetvar@kk.gov.hu

2. számú melléklet: A PSZDN archiválási osztály elemzési táblája

Szigetvári Tankerületi Központ

Az EIR-hez tartozó alapadatok 2.0 (Az EIR archiválási osztály (archiválási kategória) meghatározása kötelező!)	
Az Elektronikus Információs Rendszer neve:	KRÉTA - Poszeidon Irat és Dokumentumkezelő rendszer
EIR rövid kódja:	PSZDN
EIR állapota:	Folyamatban
Adatkezelő szervezet megnevezése:	Szigetvári Tankerületi Központ
Adatgazda neve:	Szigetvári Tankerületi Központ igazgatója
Adatfeldolgozó szervezet megnevezése:	NISZ Zrt.
Mentési osztályba sorolás dátuma:	2022.12.31.
EÜF kapcsolattartó megnevezése:	Informatikai kapcsolattartó
EÜF kapcsolattartó elérhetősége (e-mail, telefon):	Informatikai kapcsolattartó
Egy teljes mentés mérete (Mbyte-ban):	nem meghatározható, változó
Az EIR rövid leírása:	A KRÉTA - Poszeidon Irat és Dokumentumkezelő rendszerbe integrált HKP a Központi Elektronikus Szolgáltató Rendszer (központi rendszer, KR) része. 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 KRÉAT - 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 fel évente teljes állomány archiválása >Havonta változások archiválása A hatósági ellenőrzés éves ellenőrzési terv szerint
Amennyiben az adatgazda a meghatározott besorolással nem ért egyet, javasolhatja az EIR alternatív besorolását. (Amennyiben szükséges, az EIR archiválási osztályának meghatározását követően töltendő ki.)	
Az adatgazda az alábbi indoklás szerint, a fent meghatározottaktól eltérő alternatív	Az adatgazda által az EIR bizalmosságára javasolt alternatív biztonsági osztály:
Az adatgazda indoklása a javasolt archiválási osztályokhoz: (Az alternatív archiválási osztály megadását követően kötelező kitölteni!)	

