Az „Elektronikus levéltár” projekt keretében a hosszú távú levéltári megőrzéshez szükséges szabályozási feltételek kidolgozása

Az elektronikus levéltári iratok hosszú távú megőrzésével szemben támasztott követelmények

a **Magyar Országos Levéltár** részére

Változat száma:	2.0
Fájlnév:	FLX_MOLSZM_e-iratok_ht_megorzese_v2.0_110801.docx
A dokumentumot készítette:	FLEXUS Consulting Tanácsadó Kft.
Oldalak száma:	87
Mellékletek száma:	0

Minőségbiztosítás:

Dokumentum jellemzők:

Projekt megnevezése:	Az „Elektronikus levéltár” projekt keretében a hosszú távú levéltári megőrzéshez szükséges szabályozási feltételek kidolgozása
Dokumentum címe:	Az elektronikus levéltári iratok hosszú távú megőrzésével szemben támasztott követelmények
Verziószám:	v2.0
Minősítés (állapot):	Kiadva
Vonatkozó időszak:	-
Kiadás dátuma:	2011.08.01
Készítette:	Lits Bálint, Hirling László
Fájlnév:	FLX_MOLSZM_e-iratok_ht_megorzese_v2.0_110801.docx

Verziók jegyzéke:

Ver-zió	Szerző	Dátum	Változtatás rövid leírása
0.1	Lits Bálint	2011. 06. 06.	Termék annotált tartalomjegyzéke
0.2	Lits Bálint	2011. 06. 17.	Tartalomjegyzék elfogadott verziója
1.0	Lits Bálint Hirling László	2011. 07. 18.	Első véleményezésre szánt munkaközi verzió
1.3	Hirling László	2011. 07. 29.	Vélemények alapján véglegesített verzió
2.0	Hirling László	2011. 08. 01.	Dokumentum kiadása

Ellenőrizte:

Ellenőrzést végezte	Ellenőrzés dátuma	Aláírás

Jóváhagyta:

Név	Szervezeti egység/Beosztás	Dátum	Aláírás
			-

Kapják:

#	Cégnév	Név	Szervezet	Beosztás
1				
2				
3				

Tartalomjegyzék

1. BEVEZETÉS

1.1. A megbízható elektronikus levéltár

Az elektronikus levéltárak létrehozásával egyidejűleg megjelenik a rendszerek megbízhatóságára, hitelességére, fenntarthatóságára és interoperabilitására vonatkozó követelmények megfogalmazásának igénye. Az elektronikus levéltári iratok hosszú távú hitelessége és értelmezhetősége az életciklus beavatkozásainak megbízhatóságán és a beavatkozások dokumentációján alapszik. Ezeknek a követelményeknek, amelyek fontosak a hagyományos levéltári anyag őrzésekor, hatványozottan kell érvényesülniük az elektronikus iratok esetében. A digitális írásbeliség terjedésének egyik akadálya a bizalom hiánya. Annak a közmegegyezésen alapuló gyakorlatnak és tudásbázisnak a hiánya, amely alapján az elektronikus gyűjteményeket a használók megbízhatónak fogadják el.

1.1.1. AZ IRATOK HITELESSÉGE

Az írásbeliség születése szorosan összefügg a hitelességgel. A jogok írásba foglalása és az iratok jogbiztosító őrzése a levéltárak létrehozásának elsődleges oka volt, az ókori és középkori társadalmakban az emberek, városok és birodalmak feletti uralmat legitimáló szerződések, alapító okiratok, adománylevelek, kiváltságlevelek a magántulajdon és a fennálló rend garanciáját jelentették. A hitelesség kérdése a digitális információra alapuló társadalomban fokozottan jelentkezik. A levéltáraknak pontosan érteniük kell a hitelesség különböző aspektusait, hogy az általuk őrzött iratokon keresztül biztosíthassák a jogbiztonsághoz és a történeti érték megismeréséhez fűződő érdekeket.

A hitelesség vizsgálata szempontjából meg kell különböztetni az irat hitelesítését és az irat hitelességét. Az elektronikus iratok hosszú távú megőrzésének elméleti megalapozásával foglalkozó InterPares[1] projekt hitelességgel foglalkozó munkacsoportjának fontos megállapítása volt

1 Az InterPares projekt 1999-ben indított nemzetközi kutatási projekt volt a hiteles elektronikus iratok hosszú távú megőrzésének elméleti és módszertani kérdéseinek vizsgálatára (The International Research on Permanent Authentic Records in Electronic Systems). Az ausztrál, kanadai, amerikai, kínai és olasz kutatók munkáját a kanadai Vancouverben lévő University of British Columbia könyvtár- levéltár- és információtudományi tanszéke (UBC SLAIS) koordinálta, amely a modern levéltárelmélet egyik meghatározó műhelye. A projekt az elektronikus iratok inaktív (levéltári) szakaszában vizsgálta a hitelesség, iratértékelés és állományvédelem kérdéseit. A

ennek a különbségtételnek a hangsúlyozása. Míg a hitelességet az irat teljessége és a létrehozás folyamata feletti kontroll biztosítja, addig a hitelesítés azoknak a formáknak alkalmazása, amelyek valamely irat minőségét kétségtelenné teszik. A hitelesítés ezek szerint az irat egy adott időben egy hitelesnek elfogadott személy, vagy hiteleshely deklarációja arról, hogy az irat hiteles, ami írásban vagy valamilyen jelekkel hozzáadható vagy hozzáfűzhető az irathoz, tanúsítva, hogy az irat hiteles. (InterPares 2002. 21-34.o.).

Ha úgy fogjuk fel az iratot, mint olyan dokumentumot, amely egy bizonyos tevékenység során készült, ezen feladata betöltése során úgy működik, mint az adott tevékenység dokumentálása, mint a tevékenység tükörképe vagy lenyomata. Ezen funkciójának értéke - érvényessége és a bizonyító ereje - az irat hitelességétől függ. Az irat akkor hiteles, amikor maga is tényként kezelhető, mint az az esemény, amelyről tudósít. Például egy hiteles állampolgársági okirat azt jelenti, hogy az illető az adott ország állampolgára. Az iratok hitelességét e szerint a felfogás szerint nem az aláírás és a formai jegyek, hanem kizárólag az irat teljessége és a létrehozás feletti kontroll képes biztosítani. (Duranti 1995. 6.o.)

A hitelesítésnek az iratnak, mint jognyilatkozatnak az érvényessége szempontjából van jelentősége, bár ebben az esetben is csak az iratok egy részénél. A magyar eljárásjogok ugyanis a szabad bizonyítás elvének alapján állnak: ez azt jelenti, hogy a bizonyítékok mérlegelése és saját belső meggyőződésének kialakítása során a bíró nincs kötve a bizonyítás meghatározott eszközeihez. A polgári perrendtartásról szóló törvény szerint “ha törvény másként nem rendelkezik, a bíróság a polgári perben alakszerű bizonyítási szabályokhoz, a bizonyítás meghatározott módjához vagy meghatározott bizonyítási eszközök alkalmazásához nincs kötve, szabadon felhasználhatja a felek előadásait, valamint felhasználhat minden egyéb bizonyítékot, amely a tényállás felderítésére alkalmas. E rendelkezések nem érintik a törvényes vélelmeket, ideértve azokat a jogszabályokat is, amelyek szerint valamely körülményt az ellenkező bizonyításáig valónak kell tekinteni.” A büntetőeljárási kódex hasonlóan rendelkezik: “ a büntetőeljárásban szabadon felhasználható minden olyan bizonyítási eszköz és bizonyíték, amely a tényállás megállapítására alkalmas lehet; a hatóságok ezeket egyenként és összességükben szabadon értékelik, és ezen alapuló meggyőződésük szerint bírálják el”.

2001-ben lezárult projektet azóta két újabb projektszakasz követte, a jelenleg futó InterPares3 célja a kis és közepes méretű archívumok esetében az előző két projekt elméleti eredményeinek a gyakorlatba való átültetése és tananyagfejlesztés képzési programok számára. (www.interpares.org).

A szabad bizonyítás mellett ugyanakkor a jogszabályok meghatározott bizonyítási eszközöket – így a közokiratot és a teljes bizonyító erejű magánokiratot – fokozott bizonyító erővel ruháznak fel. Az okirattal bizonyítható tények esetében a bíróság az egyéb bizonyítást mellőzheti. Ppt 193. § Ezt a fokozott bizonyító erőt azonban közokirat esetében a jogszabályok nem csupán a hitelességből, hanem az eljáró szervezetből (közigazgatási szerv), annak eljárásrendjéből, illetve az okirat alaki megfelelőségéből származtatja.

A levéltár az iratokat a keletkezésük után hosszú idővel veszi át, az iratok hitelesítésének ellenőrzésére, arra, hogy egy iraton eredeti aláírás szerepel-e nincs módja. A levéltári őrzés során nem a hitelesítési információk megőrzése az elsődleges feladata, hanem az iratok integritásának fenntartása. A hitelességet a levéltár szabályozott és ellenőrzött eljárásain keresztül biztosítja.

1.1.2. AZ ELEKTRONIKUS IRATOK KÜLÖNBÖZŐSÉGE

A hitelesség kérdése fokozottan merül fel az elektronikus iratok esetében, mivel annak ellenére, hogy a jogszabályok nem tesznek különbséget az iratok tekintetében azok formája és az adathordozó tekintetében, az elektronikus iratok sajátos jellemzőkkel bírnak, aminek hatása van hitelesítésükre és a hitelességük fenntartásával kapcsolatos folyamatokra.

Egyfelől számos előnnyel rendelkeznek a hagyományos iratokhoz képest: korlátlanul kommunikálhatók, ami lehetővé teszi, a levéltári kutatás térben és időben nagyobb szabadságát, korlátlanul reprodukálhatók, ami feleslegessé teszi hagyományos iratokkal szembeni állományvédelmi megfontolásokat és a teljesen identikus másolatok egyidejű használatát. Mindezen felül pedig keresés automatizálásával olyan tartalmi feltárás lehetősége nyílik meg a kutatás előtt, ami korábban elképzelhetetlen volt.

A számos előny ellenére mégis az elektronikus iratok sajátosságai jelentik a modern levéltárak számára a legnagyobb kihívását. Szemben a megfogható és szabad szemmel olvasható hagyományos iratokkal, ezek csak közvetve, gépeken keresztül értelmezhetők, a határaik bizonytalanok, tartalmuk pedig dinamikusan változhat. Mivel az információ és az adathordozó kapcsolata laza, így az irat eredetisége nehezen bizonyítható. A hitelesség nem köthető az adathordozóhoz mivel az elektronikus médiák fizikailag instabilak, sérülékenyek és gyorsan elavulnak.

Előfordul, hogy egy irathoz tartozó adatok szétszórtan, különböző helyeken és rendszerekben vannak. Az elektronikus irat jellemzően sokkal bonyolultabb struktúrájú, mint a hagyományos. Bizonytalan az iratok állandósága, míg a hagyományos iratoknál a forma szorosan hozzátartozik a tartalomhoz (egy ügyirat fejléce, a beadvány formája stb.), az olvasás (használat) helyétől, idejétől, az olvasó személyétől stb. függetlenül azonos módon értelmezhető, azaz egyértelmű,

az elektronikus irat esetében azonban erősen függ a megjelenítésére használt eszközöktől. (Baracs et. al. 2003. 3-26.o.)

A digitális objektumok hagyományos jellemzői (tartalom, kontextus, struktúra) az elektronikus iratok esetében kiegészülnek a megjelenéssel és viselkedéssel. Az elektronikus iratok tekintetében eltérnek a levéltári beavatkozások, amelyek nem egy fizikai objektum megőrzésére, konzerválására illetve helyreállítására irányulnak mint a hagyományos iratok esetében, hanem az integritás és értelmezhetőség fenntartására. Az elektronikus iratok aktív életciklus menedzsmentet igényelnek, már kezelésük korai szakaszában és hosszú távú megőrzésük során is a rendszeres beavatkozás – aktív megőrzés – szükséges.

1.1.3. AZ ELEKTRONIKUS IRATOK HITELESSÉGE

A hitelesség kérdése az elektronikus iratok esetében az elektronikus iratok esetében azért kap nagyobb hangsúlyt, mert létrehozásuk és kommunikációjuk a megszokott, hétköznapi eszközökkel kevésbé ellenőrizhető. Számos szempontból az elektronikus irat „megfoghatatlan”.

A 2001-ben elfogadott elektronikus aláírás törvény megteremtette az elektronikus iratok hitelesítésének jogszabályi hátterét. Az elektronikus aláírás egyértelműen azonosítja az üzenet küldőjét, és biztosítja, hogy az üzenetet senki nem változtatta meg. Az elektronikus aláírás archív változata technikai értelemben alkalmas a hosszú távú megőrzésre. A rövid távon szükséges aláírásokkal szemben az archív aláírásnak olyan jövőbeli veszélyek ellen is védelmet kell biztosítania, mint az érintett hitelesítés-szolgáltatók magánkulcsainak későbbi kompromittálódása vagy a tanúsítványok és dokumentumok aláíró algoritmusainak későbbi feltörése (értve ezek alatt a lenyomat függvényt és a digitális aláírásra alkalmazott algoritmust is). A XAdES-A archív aláírás tartalmazza az aláíráshoz és az aláíráson lévő időbélyegekhez kapcsolódó minden (végfelhasználói és szolgáltatói) tanúsítvány visszavonási információit, így ezek beszerzéséhez nem szükséges később a hitelesítés szolgáltatóhoz fordulni, kizárólag csak a külső időbélyeg visszavonási állapotáért. Ha rendszeresen (amíg a korábbi időbélyeg érvényessége még igazolható) csatoljuk a XAdES-A aláíráshoz a külső időbélyeg aktuális visszavonási információit, majd újabb - jellemzően más kulccsal vagy más technológiával készült - külső időbélyeget helyezünk el az aláíráson, akkor a XAdES-A aláírás érvényessége akkor is bizonyítható, ha a belső aláírások, tanúsítványok, időbélyegek érvényessége már nem igazolható. Az archív aláírás rendszeres felül-időbélyegzésével az érvényessége bármeddig igazolható marad. A feladat költsége és bonyolultsága ugyanakkor meghaladhatja a hitelesítés fenntartásához fűződő érdeket.

A Magyar Országos Levéltár elektronikus levéltári pilot projektje már 2002-ben felhívta a figyelmet arra, hogy az elektronikus aláírásról szóló törvény önmagában nem oldja meg az elektroni-

kus iratok levéltári szempontból való “hitelességének” problémáját. A levéltár feladata azonban a maradandó értékű iratok megőrzése során túlmutat az okiratoknak és azok jogbiztosító értékének megőrzésén, sőt meghatározóan olyan iratokat érint, amelynek létrehozásával kapcsolatban az egykorú jogszabályok nem állapítottak meg formai kötöttségeket. Az Elektronikus aláírás törvényből így nem következik, hogy a Levéltári törvény által iratnak minősített elektronikus formában létező állományok hitelesek lesznek a jövőben. Az Ügyfélkapun keresztül történő azonosítás tapasztalatai azt mutatják, hogy az állampolgár-hivatal viszonyban széles körben helyettesíteni képes az aláíróeszközök használatát így részben ez az oka, hogy a levéltárak adatvagyon felmérései nem támasztják alá az elektronikus aláírásnak az iratképzőknél való széles körű használatát.

Sértetlenség

Az elektronikus iratok hitelességének biztosításának egyik pillére az iratok sértetlensége, amelyet veszélyeztetnek a nyílt csatornán való továbbítás, vagy a tárolás során az informatikai rendszerek véletlen hibái, vagy szándékos manipuláció.

A sértetlenség legegyszerűbb biztosítása hibadetektáló kódok alkalmazása, amelyek közül a legelterjedtebb az üzenet tartalmának azonosítására szolgáló különböző ellenőrző összegek (Manipulation Detection Code, MDC) kiszámítása és az irathoz csatolása. Ezek esetében a sértetlenséget az igazolja, ha az irat használatának során a használó ismételten kiszámítja az üzenethez tartozó ellenőrző összeget, és az egyezik az irattárolás során tárolt eredeti ellenőrző összeggel.

Értelmezhetőség

Az elektronikus irattal szemben támasztott elvárásunk az is, hogy értelmezhető legyen. Az értelmezhetőség jelentése ugyancsak többértelmű. Az értelmezhetőség biztosításán keresztül (1) a levéltárnak jelentéssel bíró információt kell biztosítania a felhasználók számára és (2) függetlenül az irat eredeti formájától és reprezentációjától biztosítania kell az iratok technikai értelemben vett használhatóságát. Az iratok érthetővé tétele az iratok keletkezésével egyidejűleg kezdődő és azok levéltári használata során is folyamatosan végzendő feladat, amelynek során a leíró információ tartalma bővül. Ezzel szemben a technikai értelmezhetőség fenntartása nem ritkán olyan transzfomrációkat is magában foglal, amelynek során bizonyos tulajdonságok nem tarthatók fenn. Az iratok eredeti bitsorozata azonban mindenképpen ezek közé tartozik. A bitsorozat megváltozásával az ellenőrző összeg nem bizonyítja tovább az irat sértetlenségét.A sértetlenség elve és az értelmezhetőség fenntartásának elve technikai szinten egymást kizáró köve-

telmények, ezért a levéltárnak a hitelességet biztosító tényezők összességének, az iratok integritásának fenntartására kell törekednie.

Az elektronikus iratkezelő rendszerek ezt az iratok kezelésének korai időszakában az iratkezelési folyamaton keresztül, (munkafolyamat, autentikáció, naplózás) valósítják meg. Az iratkezelési folyamat kontrollját az iratkezeléssel kapcsolatos szabályozás és szabványok és a szervezet működési rendje képes biztosítani.

Ezen túlmenően az elektronikus iratok hitelességének biztosítása során nagyobb hangsúlyt kap az iratok létrehozásának részletes dokumentációja és megfelelő metaadatokkal való ellátása. Részletesen le kell írni azt a rendszert, amelyben keletkeztek és léteztek az iratok. Pontosan rögzíteni kell a strukturális elemek, a kapcsolódó iratok (rekordok) és irategyüttesek (táblák, fájlok) közötti összefüggéseket, mivel az elektronikus iratok jellemzően bonyolult szerkezetűek, de nehezebb a szokásos kapcsolódások áttekintése is.

1.1.4. AZ ELEKTRONIKUS LEVÉLTÁR HITELESSÉGE

A levéltárak a középkorban hiteleshelyi funkciót betöltő intézményekként jöttek létre, feladatuk volt az oklevelek és kiváltságlevelek kiállítása, másolása és őrzése. A káptalanok, konventek levéltárai által őrzött és lemásolt iratokat hitelesnek kellett elfogadni. A modern levéltárak létrehozásakor is szerepet játszott a levéltári hitelesség fenntartása. „Száz oly eset fordul elő a törvényhozás, közkormányzat és igazságszolgáltatás mezején, mely századok előtti tényeken, azok iránt később költ törvényeken, okleveleken, más közhitelességű irományon alapul.” (Jakab 1877. 53.o.)

Ezért nem meglepő, hogy a levéltár hitelességét a jelenlegi jogszabályok is elismerik „bizonyító ereje van az okirat megőrzésére hivatott szerv (pl. levéltár) által vagy ellenőrzése mellett készített felvételnek vagy okiratnak”, valamint “a közokiratot kiállító vagy őrzésére hivatott szerv által a felvétel (vagy adathordozó útján nyert adatok) alapján készített kiadványnak” (Pp. 195. § (1), (2).

A levéltár feladata a hitelesség fenntartásában akkor kezdődik, amikor az archívum az iratképzőtől az iratokat átveszi. Ezt követően „az elektronikus levéltárnak biztosítania kell, hogy az általa őrzött és kutatásra bocsátott információ az, aminek látszik, hogy egy elektronikus irat bármely későbbi változata rendelkezik azzal a tartalommal, funkcionalitással és viselkedéssel, mint az eredeti példány. A hitelesség csak az átvétel szigorú ellenőrzésén és azt követően az konverziók során illetve más állományvédelmi beavatkozások során valamennyi jelentős tulajdonság megőrzésén érhető el.” (Ross és McHugh 2005)

Alapszinten a megbízható elektronikus levéltár meghatározását úgy kezdhetjük „jelenlegi és jövőbeni elkötelezettség az archívum által gondozott elektronikus iratokhoz való kiszámítható, hosszú távú hozzáférés biztosítására a felhasználók számára" (TDR 2002. 5.o.). A nestor munkacsoport[2] szerint a megbízható „hosszú távú elektronikus levéltár egy összetett és komponenseit tekintve kölcsönös kapcsolatban levő rendszer (nestor 2006. 11.o.). Mindenképpen több mint pusztán az az elektronikus megőrzési rendszer, ami a digitális anyagok kezelését végzi. A megbízhatóság meghatározása során ezért az archívumot, mint egész rendszert szükséges nézni, beleértve a szervezetet, amely az archívumot működteti, annak irányítását, szervezeti struktúráját, alkalmazottait, szabályzatait és eljárásait, pénzügyi helyzetét és fenntarthatóságát; a szerződéseket, engedélyeket és kötelezettségeket, amelyek mentén működnie kell. „A levéltárosok gyakran öröklik meg régi dolgok gondját, történelmi dokumentumokat vagy tárgyakat, ezekből mégsem lesz magától archívum. Egy valódi archívum a bizonyítékok kontextusra alapozott szerves egysége, nem pedig csupán egy rakás információ." (Muller, Feith, and Fruin 1968. 14.o.)

Emellett az elektronikus objektumkezelési gyakorlat, a technológiai infrastruktúra és a fizikai adatbiztonság ésszerű és megfelelő kell legyen, hogy az archívum hivatását és kötelezettségeit képes legyen teljesíteni. A megbízható elektronikus levéltár észleli a külső veszélyeket és a rendszeren belüli kockázatokat. Ez lehet az adathordozók, a hardverek, szoftverek sérülései, telekommunikációs problémák, a hálózati szolgáltatás hibái, a média és a hardverek elavulása, a szoftverek elavulása, a kezelők hibái, természeti katasztrófák, külső támadások, belső támadások, pénzügyi csőd, szervezeti elégtelenségek. A folyamatos ellenőrzés, tervezés és karbantartás a tudatos beavatkozással és a stratégiák végrehajtásával egyaránt szükségesek, hogy az archívumok végrehajtsák a digitális megőrzéssel kapcsolatos küldetésüket.

Ahogy az iratok hitelességét a teljesség és a létrehozás feletti kontroll, úgy a levéltári megőrzés hitelességét az integritás fenntartásának képessége és a levéltári megőrzés folyamatai feletti kontroll jelenti. Az irat integritását – sértetlenségét - a fizikai biztonság, a folyamatok és az ellenőrzőösszegek biztosítják oly módon, hogy a rendszerben kezelt adat tartalma és tulajdonságai az elvárttal megegyezzenek - ideértve a bizonyosságot abban, hogy az elvárt forrásból származik és a származás megtörténtének bizonyosságát is -, továbbá a rendszerelemek a rendelteté-

2 A megbízható elektronikus archívum tanúsításával foglalkozó nestor munkacsoport a Német Oktatási és Kutatási Minisztérium által létrehozott nestor projekt keretében jött létre, hogy összeállítsa a tanúsításhoz szükséges első követelményjegyzéket. A munkacsoport tagjai számos közösséget képviseltek, beleértve a könyvtárakat, levéltárakat, múzeumokat, kutatóintézeteket, könyvkiadókat, szoftverfejlesztőket és tanúsító testületeket. http://www.langzeitarchivierung.de/eng/

süknek megfelelően használhatóak legyenek. Az irat értelmezhetőségét a metaadatok és az állományvédelmi beavatkozások biztosítják.

A felhasznált auditálási módszertanok négy fontos ismérvet fogalmaznak meg a megbízható elektronikus levéltárral szemben: a levéltár folyamatainak dokumentáltnak, átláthatónak kell lenniük, a célnak megfelelő megoldásokat kell alkalmaznia és törekednie kell a teljesítményének mérhetőségére.

Dokumentáltság - A célokat, a terveket, a specifikációkat és a hosszú távú archívum megvalósítását megfelelően dokumentálni kell, a dokumentációt rendszeres ütemezés szerint felül kell vizsgálni.

Átláthatóság: Az archívumnak belső és külső értelemben egyaránt biztosítania kell az átláthatóságot. Csak az az archívum lehet megbízható, amelynek tervei, specifikáció, gyakorlata, szabályzatai és kockázatelemző eljárásai hozzáférhetők. Az elektronikus levéltáraknak átláthatóaknak kell lenniük valamennyi gyakorlatukat tekintve, amely érinti megőrzési lehetőségeiket, vagy az elektronikus iratok megbízható, hosszútávú megőrzésével kapcsolatban tett állításaikat. Ez az átláthatóság teszi lehetővé a kockázatok feltárását, teszi lehetővé az információval kapcsolatban érdekeltek, és felhasználók megalapozott döntéseit.

A megfelelősség elve számításba veszi, hogy nem létezik abszolút szabvány az archívum szervezeti struktúrájának, a digitális objektumkezelés, a technológiák és a technikai infrastruktúra valamennyi aspektusára. Még ha lennének is, akkor sem lennének alkalmazhatók valamennyi típusú archívum és levéltár számára minden helyzetben. Az archívum konkrét eljárásrendjének és gyakorlatának mindig az adott hosszú távú elektronikus levéltár céljain és kötelezettségein kell alapulnia.

A mérhetőség célja az, hogy legyenek objektív kritériumok, amelyekhez viszonyítva az archívumok teljesítménye értékelhető.

Jelen dokumentum ezeknek a követelményeknek a részletes kifejtését tartalmazza.

1.2. A dokumentum célja, alkalmazása

Az ajánlás az elektronikus iratokat őrző közlevéltárakkal szemben támasztott követelményrendszert tartalmazza.

A dokumentum elsősorban azzal a szándékkal készült, hogy a nemzetközileg széles körben elfogadott – mintegy szabványnak tekintett - dokumentumokra erősen építve, azokat a magyar viszonyokra adaptálva teremtse meg a hazai gyakorlat alapját. Az elektronikus iratok levéltári

megőrzésére nincs kiterjedt magyarországi gyakorlat, az iratkezelés, a levéltári intézményrendszer hazai sajátosságai ugyanakkor hatással vannak az nemzetközi gyakorlat hazai alkalmazhatóságának lehetőségeire. Ezeknek a dokumentumoknak a hosszú távú fenntartása, verziókövetése kizárólag nemzetközi szakmai közösség erőforrásaira támaszkodva, azzal szoros együttműködésben biztosítható. A nemzetközileg egységes feltételrendszernek természetesen ezen túlmenően is számos előnye van. A TRAC szerzői is olyan követelményrendszert vizionáltak, amely „nemzetközi környezetben valósul meg, közös kritériumkészlettel, de regionális megvalósítással pl. országonként, földrészenként vagy földrajzi térségenként."

Ez a dokumentum azoknak készült, akik levéltárakban dolgoznak, és feladataik az elektronikus iratok hosszú távú megőrzésének megvalósításával függnek össze. Nem levéltárépítési kézikönyvnek készült, de a követelmények fontos útmutatást adhatnak az elektronikus iratok levéltári megőrzésével kapcsolatos feltételek és folyamatok kialakításához is.

A magyarországi közlevéltárak méretüket, feladatkörüket, levéltári anyagukat és személyi állományukat tekintve jelentősen különböznek. Jelen követelmények megfogalmazásakor figyelemmel kellett lenni arra, hogy a követelmények valamennyi közlevéltárra érvényesíthetők legyenek. A követelmények szándékosan magas szintűek annak érdekében, hogy elkerüljék azt, hogy a követelményeket különböző módon teljesíthető szervezeti, működési implementációkat kizáró előírásokat tartalmazzanak. A levéltár funkciói szerint tételekre bontott követelmények és azok magyarázatai segítenek az elektronikus levéltár tervezésében és működési gyakorlatának ellenőrzésében.

Ezen túlmenően az iratképzők és a levéltárhasználók is sok hasznos információt találnak a követelmények között, ami segítheti számukra annak megértését, mit várhatnak a levéltártól, amellyel iratátadóként vagy kutatóként kapcsolatba kerülnek. Néhány iratképző számára abban is segítséget nyújthat, hogy korszerűsítse a levéltárral való kapcsolattartást akár az iratkezelési folyamatban való tanácsadást, akár az iratátadás előkészítését tekintve.

A követelmények érintik az elektronikus levéltári funkciók valamennyi szintjét, így a dokumentum releváns valamennyi alkalmazott és a levéltár egészére tekintve is, illetve abban az esetben – egyetemi levéltárak -, amennyiben a levéltár egy nagyobb szervezet része. A szervezet vezetősége és a szabályzatok készítői számára legalább a szervezeti vonatkozású fejezetek követelményeivel kell tisztában lenni. A rendszer- és hálózatüzemeltetési személyzet számára, akik az infrastruktúráért felelősek, a műszaki és biztonsági pontok fontosak, csakúgy mint az épületbiztonságért és a tűzvédelemért felelős munkatársaknak. Az iratátvétellel és a kutatók kiszolgálá-

sával foglalkozó levéltárosok számára fontos követelményeket a Digitális tartalomkezelés fejezet tárgyalja.

1.3. Terminológia

Nemzetközi szinten az elektronikus iratok megőrzésben számos különböző közösség érdekelt, mindegyikük elkülönült szóhasználatot alakított ki a kulcsfogalmak helyi definíciójával. Még a levéltári területen is több konkurens fogalomkör létezik: az OAIS referenciamodell (OAIS 2002, ld részletesebben. 1.5.3) fogalomhasználata különbözik a Nemzetközi Levéltári Tanács definícióitól; komoly egyeztetési nehézségek vannak a hagyományos levéltári fogalmak és a magyar jogszabályok terminológiája között is, ezért fontos néhány kulcsfogalom használatára felhívni a figyelmet.

A közlevéltárak esetében az elektronikus iratok megőrzésével kapcsolatos funkcionalitás nem érinti a levéltári intézmény egészét. Jelen követelményjegyzék egyes követelményei a levéltár egészére vonatkoznak, mások pedig kifejezetten az elektronikus levéltári funkcionalitással kapcsolatosak. Ezért indokolt a két fogalmat megkülönböztetni.

Általánosságban, jelen dokumentum számos alapfogalmat vett át az OAIS referenciamodellből. Az OAIS referenciamodell egyik nagy erőssége, hogy angol nyelvterületen mára széles körben elfogadott terminológiát vezetett be, olyan fogalmakból építkezve, amelyek „nem lettek túlterhelve többféle jelentéssel, ily módon korlátozva, hogy szándékolatlan jelentéseket hordozzanak” (OAIS 2002. 1-7.o.). Mivel az OAIS alapvető dokumentuma lett az elektronikus iratok megőrzésének, a közös fogalmak könnyen érthetők így ezért használjuk őket ebben a dokumentumban is.

Az adaptáció nehézségét jelenti, hogy a nemzetközi – meghatározóan angolszász – terminológiában alkalmazott fogalmak tükörfordításai nem esnek egybe a magyar szaknyelv által leírt fogalmakkal. Így az archive szó egyaránt fordítható archívumnak, irattárnak, levéltárnak, mivel a magyar nyelv ezeket az entitásokat megkülönbözteti.

Az OAIS referenciamodell a digitális archívum [digital archive] fogalmat használja a digitális megőrzésért felelős szervezet értelemben. Jelen dokumentumban az elektronikus levéltár kifejezés hordozza ugyanazt a tartalmat minden előfordulásakor a közlevéltár elektronikus iratokat megőrző funkcionalitásának leírására.

A fogalmak magyarázata a függelékben található. Az Elektronikus Levéltári Projekt során létrehozott valamennyi szabályozási termékhez közös fogalomtár és a fogalmak összefüggéseit leíró fogalomtérkép készül.

A jelen dokumentumban használt fogalmak meghatározásait az 1. függelék tartalmazza.

1.4. Dokumentum hatóköre

Az ajánlás a magyarországi közlevéltárakra és a közlevéltárak elektronikus levéltári anyagának megőrzésére vonatkozik, de hasznos lehet valamennyi hasonló tevékenységet végző intézmény számára. A követelmények nem vonatkoznak az Elektronikus Levéltár Projekt keretében létrejövő e-irattár szolgáltatásra.

A dokumentum nem tárgyalja a minősített iratok levéltári kezelését és az elektronikus aláírás archiválását.

A levéltárnak az iratok hitelességére a létrehozás, ügyintézés, irattározás során nincs befolyása, a hitelességet csak az iratok befogadásától kezdődően tudja biztosítani. Jelen ajánlás nem a dokumentum szintű hitelességet biztosító elektronikus aláírás levéltári megőrzésével kapcsolatban kíván szabályokat megállapítani, hanem azt a követelményrendszert tartalmazza, amelynek segítségével a közlevéltár intézményi szinten képes fenntartani az általa őrzött levéltári anyag hitelességét.

Jelen ajánlás ezt elfogadva egyfelől az átjárhatóság érdekében rendre meghivatkozza azokat a követelményeket, amelyeket a kapcsolódó nemzetközi és hazai szabványok és mértékadó dokumentumok megfogalmaznak, ugyanakkor kiegészítésekkel él azokon a pontokon, amelyeken az Elektronikus Levéltár projekt során kiemelkedő igény mutatkozott. Ezek elsősorban az információbiztonság és a több szervezet azonos erőforráson működő archívumával szembeni speciális követelmények során jelennek meg.

1.5. A követelmények kialakításakor figyelembe vett szabványok, ajánlások, dokumentumok

1.5.1. NEMZETKÖZI TAPASZTALATOK

Számos modell és dokumentum készült abból a célból, hogy meghatározza azokat a jellemzőket és követelményeket, amelyek elvárhatók egy elektronikus archiválást végző intézménytől. A Nyitott Archívum Információs Rendszer (Open Archival Information System, OAIS) referencia modell megfogalmazta a magas szintű modelljét és jellemzőit azoknak az archívumoknak, amelyeknek működésük során biztosítaniuk kell a digitális információnak egy meghatározott közönség számára való fenntartását. Az OAIS modell elterjedését követő erőfeszítések azt célozták meg, hogy meghatározzák azokat a követelményeket, amelyek birtokában egy archívum képes az OAIS-ban megfogalmazott funkcionalitást megbízhatóan teljesíteni. Ennek első kísérlete a „TDR jelentés” címen ismertté vált kutatás volt, amelyet egy könyvtári módszertani konzorcium,

a Research Library Group és az Online Computer Library Center készített. A jelentés meghatározta a megbízható elektronikus levéltárat és annak főbb jellemzőit, továbbá megfogalmazta egy ehhez kapcsolódó auditálási eljárás szükségességét. Ennek eredményeként az RLG már az Egyesült Államok Szövetségi Levéltárával (National Archives and Records Administration) közös munkacsoportban arra vállalkozott, hogy egy olyan szabványt hozzon létre, amely érvényes a digitális archívumok mind szélesebb körére, amelyek digitális archiválási szolgáltatást nyújtanak „megbízhatóan tárolva, konvertálva, hozzáférhetővé téve a digitális gyűjteményeket." Ennek a munkának lett eredménye 2007-ben a TRAC dokumentum, amelyre jelen ajánlás erősen támaszkodik. (*Trustworthy repositories audit & certification: Criteria and checklist*. <http://www.crl.edu/PDF/trac.pdf)

A TRAC dokumentumra számos további alkalmazása épült.

A Massachusetts Institute of Technology (MIT) PLEDGE projektjének célja az volt, hogy egyértelmű listát hozzon létre azokból a szabályzatokból – szabályozási területekből - amelyet egy intézményi archívumnak létre kell hoznia és végrehajtania, hogy kielégítse a NARA TRAC követelményeit. 2007 januárjában az angol Digital Curation Center, a Digital Preservation Europe projekt, a német NESTOR projekt és a Center for Research Libraries (CRL) képviselői meghatározták a digitális archívum tíz alapvető – magas szintű kritériumát.

- Az archívum elkötelezett a digitális objektumok folyamatos fenntartására a meghatározott levéltárhasználók érdekében.
- Képes demonstrálni szervezeti életképességét (pénzügyi, személyzeti és eljárási tekintetben is), hogy elkötelezettségét megvalósítsa.
- Megszerzi és fenntartja a szükséges szerződésbeli és törvényi jogait és teljesíti a kötelezettségeit. Hatékony szabályozási keretekkel rendelkezik.
- Hatékony és hatásos szabályzatokkal rendelkezik
- Megállapított követelményeken keresztül gyarapítja és veszi át a megőrzendő iratokat.
- Fenntartja és biztosítja az iratok integritását, hitelességét és használhatóságát az idők során.
- Létrehozza és fenntartja a szükséges metaadatokat a digitális objektumokon végrehajtott beavatkozásokról, az iratok létrehozásáról, hozzáféréséről és a megőrzést megelőző használatról.
- Teljesíti a szükséges kutatószolgálati követelményeket.
- Stratégiai tervvel rendelkezik a megőrzéstervezéssel és az állományvédelmi beavatkozásokat illetően.

- Megfelelő technikai infrastruktúrával bír a digitális objektumok folyamatos megőrzéséhez és a biztonsági követelmények teljesítéséhez.

(Ten principles)

Az amerikai TRAC és a vele párhuzamosan és szoros kapcsolatban dolgozó német Nestor projekt tapasztalatait használta fel a digitális archiválás kutatásában két élenjáró szervezet a Digital Curation Centre (DCC) és a DigitalPreservationEurope (DPE) audit-módszertanuk fejlesztésekor. A Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) [Kockázatelemzésen Alapuló Digitális Irattár Audit Módszertan], a DCC által 2006 és 2007 során végrehajtott kísérleti auditok tapasztalatain alapul. Az alapvetően önértékelésre fejlesztett módszertan a digitális archívumokkal rendelkező intézmények, összevethető, mérhető alapokon nyugvó teljesítményértékelését támogatja. Az eszközzel mérhető, hogy a szervezetek mennyire képesek felismerni, azonosítani, értékelni és kezelni a megőrzést befolyásoló kockázatokat. A hat lépésből álló audit segíti az archívum erőforrásainak hatékony felhasználását, a szervezet irányítása számára a kockázatok azonosítását és besorolását, aszerint, hogy melyek azok, amelyektől a leginkább kell tartani, akár azért, mert bekövetkezésük igen valószínű, akár azért, mert a legnagyobb hatást gyakorolja az archívumra.

A követelmények szerkezete igyekszik követni a forrásként felhasznált nemzetközi szabványokat, de a hazai viszonyokra való adaptálás olykor a követelmények összevonását vagy a nagyobb hangsúly érdekében egy követelménynek a szétbontását tette szükségessé.

1.5.2. HAZAI ADAPTÁCIÓK

Ez idáig nem készült olyan hazai, általánosan elfogadott követelményrendszer, mely jelen dokumentum meghatározó forrása lehetne.

A megbízható elektronikus levéltárak követelményeihez leginkább közel álló megoldás az elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható működésének kialakítására és a megfelelőség ellenőrzésére a Nemzeti Hírközlési Hatóság által kidolgozott két követelményrendszer. A „Biztonsági követelmények elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható rendszereire” című dokumentum az ISO 14721:2002 (OAIS) és az ISO 17799:2006 szabványokra építve az archiválás szolgáltatás megbízható rendszereinek műszaki követelményeit tartalmazza, összhangban az „Eljárásrendi követelmények elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható rendszereire”, mely az archiválási szolgáltatók működésére (eljárásrendjére, szabályzataira) vonatkozik. A két követelményrendszer az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eat.) szerinti archiválási szolgáltatók megbízható működésének

kialakítására és megfelelőségük ellenőrizhetősége szolgál, célja ugyan nem a maradandó értékű iratok megőrzése, hanem az elektronikus aláírás felhasználásával megvalósított elektronikus archiválási szolgáltatások működésének megalapozása, de az alapelvek megegyeznek a levéltári archívummal.

1.5.3. SZABVÁNYOK

- ISO 14721:2003 - A nyitott archívumok referencia modellje (Open Archival Information System, OAIS) az elektronikus archiválás uralkodó szabványa. Ismerteti a legáltalánosabb fogalmakat, a legátfogóbb iratátvételi, ellenőrzési, archiválási, hozzáférési folyamatokat, a felelősségi köröket, a metaadatok típusait. Koncepciója kiterjed az elektronikus és papír alapú iratokra is. A folyamatok mellett kiemelt szerepe van a szervezetre és a felelősségi körökre vonatkozó követelményeknek és az információs modellnek. A követelményeit magas szinten fogalmazza meg, ezért egyaránt alkalmas magán- és tudományos archívumok, valamint közlevéltárak megalapozására. Sem a tárolás, sem az adatcsere konkrét formáiról nem tesz állításokat, a legtöbb területen csak a kezelendő problémákat és magas szintű megoldási sémáikat tárja fel, a konkrét megoldásokat már a bevezető intézmény belső szabályozási rendjébe sorolja, azonban a választott stratégiák és megoldások dokumentációs kötelezettségét előírja.
- MSZ ISO/IEC 27001:2006 - Az információbiztonság irányítási rendszerei. Az információbiztonsági szabályzat szükségességét fogalmazza meg, és célja, hogy egy szervezeten belül világos menedzsmentet és irányítást nyújtson. Ebben a dokumentum azok a követelményei jelennek meg, amelyeket egy archiválási szolgáltatónak érvényre kell juttatnia az információbiztonsági szabályzatán keresztül.
- MSZ ISO/IEC 17799:2006 - Az informatikai biztonság menedzselésének eljárásrendje. Ez a szabvány azoknak ad informatikai biztonságmenedzselési ajánlásokat, akik saját szervezetük körében a biztonság kezdeményezéséért, megvalósításáért és megtartásáért felelnek. Arra tervezték, hogy közös alapot szolgáltasson a fejlődő szervezetek biztonsági szabványaihoz és hatékony biztonságmenedzselési gyakorlatához.

2. KÖVETELMÉNYEK

2.1. Szervezeti és folyamat-követelmények

Bár az elektronikus iratok természetéből fakadóan a technológia meghatározója egy elektronikus levéltárnak, az eszközök csak egyik területét jelentik az elektronikus levéltár funkcióit támogató infrastruktúra egészének. Az archívum egy szervezet keretében működik, amelyet meghatároznak a szervezet céljai, a jogszabályi környezet, az intézmény munkatársai és a rendelke-

zésre álló költségvetés. A közlevéltár szervezeti jellemzői ezért legalább annyira fontosak, mint rendszer hardver- és szoftverkomponensei. Hatással vannak a teljesítményre, a kiszámíthatóságra és fenntarthatóságra.

Azokat a követelményeket, amelyek ezeket az elemeket érintik, öt csoportba soroltuk.

- Szervezeti keretek (SZK)
- Irányítás (IR)
- Szervezet, feladat- és hatáskörök, munkatársak (SZERV)
- A folyamatok kiszámíthatósága és szabályozása (KSZ)
- Fenntarthatóság (FENNT)

2.1.1. SZERVEZETI KERETEK (SZK)

2.1.1.1. A levéltárnak legyenek írásban rögzített intézményi szintű céljai, amelyek tükrözik elkötelezettségét a digitális információ megőrzésére, kezelésére és hozzáférésének biztosítására (SZK_CEL)

A levéltár céljai legyenek világosan értelmezhetők és hozzáférhetők az iratátadók, levéltárhasználók és egyéb érdekeltek számára. A levéltárnak meg kell határoznia gyűjtőkörét, az iratok megőrzésével és hozzáférésével kapcsolatos céljait. Az általános levéltárak és a szaklevéltárak többségét tekintve ezeket a célokat, a levéltár illetékességét a Levéltári törvény és a 10/2002. (IV. 13.) NKÖM rendelet, valamint a levéltárak alapító okiratai pontosan megfogalmazzák. Más esetekben ezeket a célokat a fenntartó határozhatja meg.

A célok illeszkedjenek az intézmény feletti közigazgatási vagy ágazati célokhoz (Pl. Levéltárak középtávú informatikai stratégiája és feladatterve 2006-2010). [TRAC A1.1, Nestor 1.1, PLEDGE OEL-0001]

2.1.1.2. Az elektronikus levéltár biztosítsa a hatályos jogszabályoknak való megfelelőséget az iratátvétel, archiválás és használatra bocsátás során. (SZK_JOGSZ)

Az elektronikus levéltár tevékenysége feleljen meg a jogszabályoknak. A közlevéltárak tevékenységét számos jogszabály érinti, előírva a maradandó értékű iratok megőrzését, a köziratok nyilvánosságának biztosítását, a személyes adatok védelmét, a szerzői jogok érvényesítését, a történelmi múlt megismeréséhez való jog biztosítását. A jogszabályokon túlmenően a közlevéltárakra egyéb kötelezettségek is hárulnak kétoldalú szerződésekből eredően, ilyenek például a letéti megállapodások, ajándékozási szerződések. A levéltárak a nem közfeladatot ellátó szervekkel az iratkezelés ellenőrzésére, tanácsadásra is szerződést köthetnek. A levéltárnak a jogszabályokból és szerződésekből fakadó kötelezettségeit a tevékenységében közreműködő szervezetek esetén az együttműködési megállapodásokon, szolgáltatási szerződéseken keresztül is biztosítania kell. [Nestor 3.1, 3.2, 3.3, RPJ 2.3.1, PLEDGE OEL-0002]

2.1.1.3. Az elektronikus levéltár méretére, illetékességére vagy anyagára való tekintet nélkül mutasson fel explicit, megfogható, hosszú távú elkötelezettséget a meghatározó szabványoknak való megfelelésre. (SZK_SZABV)

A szabványosság a korszerű rendszerekkel szemben támasztott alapvető követelmény. Szabványosság nélkül sem megfelelő levéltári megoldás, sem jól használható informatikai megvalósítás nem létezik. Az elektronikus levéltárnak törekednie kell a tevékenységét érintő szabványoknak, mértékadó dokumentumoknak, archiválási tapasztalatoknak való megfelelésre.

Az elektronikus levéltárak területén meghatározó az OAIS szabvány (ISO 14721:2003), a levéltári anyagok összefüggéseinek leírására a Nemzetközi Levéltári Tanács szabványai, az iratkezelés területén a 15489:2001, az információbiztonság területén a 27001:2006 és a 17799:2006 szabványok, stb.. A dokumentált, nyílt szabványok alkalmazása hozzájárul az archívum működésének átláthatóságához, nyomon követhetőségéhez és megbízhatóságához.

2.1.1.4. A levéltár rögzítse levéltári anyaga kiválasztásának alapvető elveit (SZK_KIV)

A levéltárnak írásban rögzítenie kell, hogy milyen iratok tartoznak a gyűjtőkörébe. Ezt gyakran jogszabályok (Ltv.) vagy a fenntartó határozza meg.

A levéltári törvényből következőkön túlmenően a levéltárnak meg kell határoznia gyűjteménye gyarapításának elveit, a maradandó érték meghatározásának módját. Ennek módja lehet gyűjtőterületi politika készítése vagy a levéltár célját meghatározó dokumentumokban a gyűjtemény határainak definiálása. A gyűjtőterületi politika célja, hogy a levéltár intézményi céljával összhangban meghatározza azokat a konkrét szempontokat, amelyeket a levéltár az iratértékelésnél, az irattári tervek maradandó értékű tételeinek meghatározásásán keresztül az iratok megőrzésre való kiválasztásánál figyelembe vesz .

Pl.:

- Az Ausztrál Kulturális Miniszterek Tanácsának nemzeti örökség megőrzési programja:

  http://www.nla.gov.au/preserve/cult.html#back

- A Svéd Királyi Levéltár iratértékelési politikája:

  http://www.riksarkivet.se/default.aspx?id=10854&ptid=0&column=title&value=Appraisal+policy

- Az Egyesült Királyság Levéltárának gyűjtőterületi politikája:
  http://www.nationalarchives.gov.uk/recordsmanagement/acquisition-disposition-strategy.htm
- London Város Levéltárának iratértékelési politikája:

  http://www.history.ac.uk/gh/apppol2008.pdf

[Nestor 1.2]

2.1.2. IRÁNYÍTÁS (IR)

2.1.2.1. A levéltár rendelkezzen az elektronikus iratok megőrzésével kapcsolatos hosszú távú tervekkel. (IR_STRAT)

Az elektronikus iratok megőrzésével kapcsolatos feladatok természetéből következik, hogy a levéltárnak szükséges hosszú távú terveket készítenie azzal kapcsolatban, hogy hogyan kívánja elérni az (SZK_CEL) követelmény alapján megfogalmazott céljait. A tervek fedjék le az intézmény ismert és várható feladatait, kötelezettségeit és az előírt határidőket.

A hosszú távú tervezés alapját az intézményi célok, a szervezeten belüli ellenőrzések, és a technikai és társadalmi környezet változásainak követése jelentik. Így ide értendő az OAIS követelménye a levéltárhasználói csoportok igényeinek követésével kapcsolatban (monitoring designated community) vagy az OAIS technológiafigyelés funkciója (Technology Watch). Az Ügyfélkapu használatának terjedése vagy a tanúsított iratkezelő szoftverek követelményeiben való változások éppúgy közvetlenül hathatnak az elektronikus levéltár működésére, mint egy új eszköz vagy fájlformátum megjelenése. A stratégiai tervezésnek igazodnia kell az intézményi szintű célokhoz (SZK_CEL) és figyelemmel kell lennie a feladatokhoz biztosítandó erőforrásokra (FENNT_FIN) [Nestor 4.4]

2.1.2.2. A levéltár rendelkezzen rendszeres minőségellenőrzési ütemtervvel és törekedjen a működésével kapcsolatos tanúsítványok beszerzésére / fenntartására. (IR_TAN)

A levéltárnak rendszeres, dokumentált és átlátható módon kell megvalósítani az elektronikus levéltár működési folyamatainak ellenőrzését. Az átfogó intézményi célokat [lásd SZK_CEL] specifikus célokra és konkrét feladatokra kell lebontani. Az ellenőrizhetőség érdekében az értékelése során mérhető mutatókat kell alkalmazni.

A megbízható elektronikus levéltár működésében a dokumentáltság kiemelkedően fontos, az ellenőrzés során ezért kiemelt szerepet kell, hogy élvezzen a folyamatok dokumentáltsága, a dokumentumok naprakészsége, teljessége és pontossága. Biztosítani kell az egyes dokumentumok változáskezelését, különös tekintettel a hardver- szoftverdokumentációra és a digitális objektumok kezelésével összefüggő dokumentációra.

Az elektronikus levéltárnak törekednie kell arra, hogy objektív, külső, állandó és megismételhető tanúsítási folyamatokkal biztosítsa és demonstrálja, hogy az elektronikus levéltár teljesíti és várhatóan a jövőben is teljesíteni fogja a megbízható archiválás követelményeit. A külső szervezetek tanúsításai a legjobb fokmérői annak, hogy az elektronikus levéltár teljesíti a követelményeket, betölti a szerepét, tevékenysége illeszkedik a megfelelő szabványokhoz. Az elektronikus

levéltárnak törekednie kell arra, hogy működésébe és tervezési folyamataiba integrálja a külső tanúsítások megvalósítását.

A tanúsítás vonatkozhat a megbízható elektronikus levéltár egészére, vagy a szervezetre (minőségirányításra tanúsítás), az információbiztonságra, illetve a működéshez szükséges egyes komponensekre (így pl. a gépterem, tűzvédelem, árnyékolás, betörés elleni védelem tanúsítása).

Például:

- ISO 9001:2008 – Minőségirányítási rendszerek,
- ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei.
- MSZ EN 1047-2:2002 Biztonságos értéktároló eszközök. Tűzállósági osztályozás és vizsgálati módszerek. 2. rész: Adattároló termek és adattároló konténerek

[TRAC A3.9, Nestor 5.2, PLEDGE OEL-0010, OEL-0011, OEL-0012]

2.1.3. SZERVEZETI FELÉPÍTÉS, FELADAT- ÉS HATÁSKÖRÖK, MUNKATÁRSAK (SZERV)

A levéltárnak világosan és pontosan dokumentálnia kell az elvárásokat, döntéseket, fejlesztéseket és tevékenységeket, melyek az általa gondozott digitális tartalom hosszú távú megőrzését és hozzáférését biztosítják. Ez a dokumentáció biztosítja mind a levéltárhasználók, mind az iratképzők számára, hogy a levéltár teljesíti az előírásokat és a megbízható elektronikus levéltárral szembeni elvárásokat.

A levéltárnak az elektronikus iratok megőrzéséhez megfelelően képzett alkalmazottakkal kell rendelkeznie és támogatnia kell folyamatos továbbképzésüket. A levéltárnak dokumentálnia kell a szükséges készségek, szerepek meghatározását és az alkalmazottak részletes munkaköri leírását.

2.1.3.1. Az elektronikus levéltár szervezeti formája és struktúrája legyen megfelelő feladatai ellátásához (SZERV_STRUKT)

Az elektronikus levéltár szervezeti felépítését oly módon kell illeszteni az intézmény egészéhez, hogy képes legyen megvalósítani mind napi, mind hosszú távú feladatait. Ez történhet önálló szervezeti egység felállításával, kisebb nagyobb mértékű szervezeti elkülönüléssel vagy a hagyományos szervezeten belüli specializált munkakörök kialakításával.

A szervezeti felépítésen és a munkakörök kialakításán keresztül is biztosítani kell a vegyes iratok megfelelő kezelését is.

A feladatok származhatnak a jogszabályi követelményekből, a szabványokhoz való illeszkedésből, mint például az OAIS követelménye a levéltárhasználói csoportok igényeinek követésével kapcsolatban (monitoring designated community) vagy az OAIS technológiafigyelés funkciója (Technology Watch)., illetve lehetnek az eredményei a levéltár letéti vagy szolgáltatási megállapodásainak [Nestor 4.3, 4.4, RPJ 2.3.1].

2.1.3.2. A levéltárnak az elektronikus iratok megőrzésével kapcsolatos feladataihoz határozza meg azokat a szerepeket, a szerepekhez kötődő készségeket illetve azokat a munkaköröket, amelyekben a megfelelően képzett és tapasztalt alkalmazottak a feladatokat elvégzik. (SZERV_SZEREP)

A levéltárnak meg kell határoznia azokat a kompetenciákat és készségeket melyek a feladatok ellátásához és a hosszú távú működtetéshez szükségesek. Biztosítania kell, hogy az alkalmazottak rendelkezzenek a megfelelő készségekkel, pl. levéltári képzettség, technikai, informatikai készségek, jogi szakértelem.

A szerepköröket arra való tekintettel kell kialakítani, hogy mind a levéltári anyag, a mind a levéltár szolgáltatásai, mind pedig a személyi állomány összetétele változni fog. Egy kis levéltár esetében halmozódnak az egyes munkatársak által betöltött szerepek, a nagyobb levéltárban lehetőség van nagyobb mértékű specializálódásra, munkamegosztásra és a felelősség nagyobb mértékű elhatárolására.

A szerepek között a hagyományos levéltári szereposztáson túl szükségképpen megjelennek új minőségek. Az elektronikus iratok kezelése két szakterület találkozásaként valósul meg. A kompetenciák egyrészt a levéltári szakmai ismeretekből, másrészt az informatika területéről származnak. Az elektronikus levéltárban dolgozó levéltárosok ismeretei kiegészülnek, a hagyományos levéltárosi ismeretekhez hozzáadódnak az elektronikus iratokhoz kötődő speciális formátumok és technikai jellemzők kezelésének módszerei. Az itt dolgozó informatikusok pedig levéltár-informatikai ismeretek megszerzésével képesek együttműködni a levéltár-szakmai szereplőkkel.

A szerepek megformálása a levéltár egészének a feladata. Általánosságban, valamennyi levéltárnak kell megoldással rendelkeznie valamennyi szerepre. Ez történhet a meglévő munkakörökhöz (gyűjtőterület, állományvédelem, informatika) kapcsolódóan, a munkaköri leírások kiegészítésével. Lehetséges egyes szerepeket a levéltárak között erőforrás-közösséggel, vagy - az informatikai szerepkörök területén (üzemeltetés, fejlesztés) - igénybevett szolgáltatáson keresztül biztosítani. Vannak azonban olyan különleges vagy szórványosan jelentkező feladatok, ahol az intézmények egymás között oszthatnak el bizonyos szerepeket. A nagyobb levéltárak illetékességébe tartozó iratképzők számossága miatt ezeknél jelentős gyakorlati tapasztalat gyűlik

össze az elektronikus iratanyag előforduló típusairól és azok kezelésének technikáiról. Ebből következően létrejönnek olyan kompetenciák, amelyek megosztása indokolt lehet, így a kisebb levéltárak számára szakmai háttérként szolgál. Az elektronikus iratok megőrzéséhez a következő szerepkörök feltétlenül szükségesek:

a) Szükséges egy szerepkör, amely biztosítja a levéltári anyaggal kapcsolatos munka irányítását.

b) Szükséges egy szerepkör, amelyen keresztül biztosítható a levéltár technikai infrastruktúrájának stratégiai fenntartása, a továbbfejlesztések előkészítése és koordinálása, az elektronikus levéltár informatikai koncepciójának érvényesítése és felülvizsgálata. Ezen a szerepkörön keresztül biztosítható vagy önálló szerepkörként definiálható az elektronikus levéltárban őrzött objektumok kezelésének informatikai irányítása, a digitális objektumok formátumai kezelésének technikai irányítása, a metaadatokat tartalmazó adatbázisok fenntartása, az állományvédelmi beavatkozások tervezése. Ezen szerepkörön keresztül biztosítható az elektronikus levéltári funkcionalitást kiszolgáló hardverek és szoftverek üzemeltetésének irányítása. Ehhez a szerepkörhöz tartozik a technikai támogatást végző munkatársak feladatainak megszervezése és ellenőrzése, a rendszer erőforrásainak felügyelete, a tervezhető karbantartási feladatok előkészítésének irányítása, az ad hoc beavatkozások szabályainak kidolgozása és a végrehajtás ellenőrzése.

c) Szükséges egy gyűjtőterületi szerepkör, amely a levéltári anyag gyarapítása forrásainak aktív feltárását biztosítja.

d) A közlevéltárakban szükséges egy szerepkör, amely a köziratok kezelésének levéltári felügyeletét, az iratkezelési szabályzatok, selejtezési jegyzőkönyvek, illetékességi iratátadások levéltári előkészítését biztosítja. A szerepkörhöz kötődő fontos kompetenciát jelentik az elektronikus iratok formátumairól és kezelésük technikai részleteiről való ismeretek.

e) Szükséges egy elektronikus állományvédelmi szerepkör. Az elektronikus iratok kezelésénél az állományvédelmi feladatok jellege eltér a hagyományos állományvédelmi feladatoktól, mivel az elektronikus iratok értelmezhetőségét is biztosítania kell. A szerepkörhöz tartozik a megőrzési stratégiák, megőrzési tervek és útvonalak kialakítása,az információs csomagok típusainak tervezése, az alkalmazott módszerek ellenőrzése és szükséges revíziója, az eljárások dokumentálása.

f) Szükséges egy szerepkör, amely biztosítja a levéltárba adott iratok befogadásának és feldolgozásának megvalósítását.

g) Szükséges egy szerepkör, amelyen keresztül biztosítható a levéltári anyaghoz való rendszeres vagy egyéni kérésen alapuló hozzáférés.

h) Szükséges egy szerepkör, amely az érdekeltek (iratképzők, felhasználók) számára a szolgáltatásokkal és azok igénybevételének szolgáltatási és technikai aspektusaival kapcsolatos információt nyújt személyesen vagy e-mail, esetleg telefon útján.

i) Szükséges egy üzemeltetői szerepkör, amelyen keresztül a levéltár biztosítja az elektronikus levéltári funkcionalitást kiszolgáló hardverek és szoftverek üzemeltetését, az automatikus folyamatok ellenőrzését, a tervezhető és eseti karbantartási feladatok elvégzését.

j) Szükséges egy informatikai fejlesztői szerepkör, amelyen keresztül biztosítható, hogy az elektronikus levéltár egyes fejlesztési feladatokat maga végezzen el. [TRAC A2.1]

2.1.3.3. A levéltár biztosítsa az egyes szerepekhez illetve munkakörökhöz tartozó feladatok és felelősségek pontos elhatárolását (SZERV_SZETV)

A levéltárnak rendelkeznie kell részletes szabályozással, amely magában foglalja a kompetencia-meghatározásokat, munkakör-definíciókat és munkaköri leírás típusokat. Ezeket a dokumentumokat rendszeresen felül kell vizsgálni a követelmények változásának megfelelően. [TRAC A2.1]

2.1.3.4. A levéltár biztosítsa a feladatok és a felelősségek egyértelmű hozzárendelését a levéltár alkalmazottaihoz. (SZERV_FELEL)

Az elektronikus levéltárnak biztosítania kell, hogy valamennyi folyamat és azok összefüggései egyértelműen meghatározásra kerültek a vonatkozó szabályzatokban, különös tekintettel arra, hogy a munkatársak egyértelmű feladatokkal és felelősségi körökkel rendelkezzenek ezeknek a folyamatoknak a végrehajtása során. Ez a követelmény akkor is fennáll, ha az elektronikus levéltár egyes feladatait külső közreműködők segítségével valósítja meg. [Nestor 5.1]

2.1.3.5. Az elektronikus levéltár rendelkezzen megfelelő számú alkalmazottal az összes funkció és szolgáltatás megvalósításához (SZERV_LETSZ)

A levéltárnak meg kell határoznia az alkalmazottak szükséges létszámát és a feladatok ellátásához a szükséges képességek (képzettség, tapasztalatok) szintjét. Az elektronikus levéltár alkalmazotti létszáma legyen arányban a jogszabályokban, a levéltári átadási megállapodásokban, szolgáltatási szerződésekben, munkatervekben, célkitűzésekben rögzített kötelezettségeivel. [TRAC A2.2, Nestor 4.2, PLEDGE OEL-0009]

2.1.3.6. A levéltár rendelkezzen továbbképzési programmal az elektronikus levéltár alkalmazottai ismereteinek bővítésére és szakértelmük továbbfejlesztésére (SZERV_KEPZ)

A technológia folyamatosan fejlődik, ezért az elektronikus levéltárnak biztosítania kell, hogy az alkalmazottak szaktudása és készségei is fejlődjenek, ideális esetben az élethosszig tartó tanulás megközelítést érvényesítve az alkalmazottak továbbképzése és megtartása érdekében. Mivel a követelmények és elvárások, melyek minden egyes funkcionális területre vonatkoznak folyamatosan fejlődnek, az elektronikus levéltárnak szakmai továbbképzési tervvel és az ehhez rendelt költségvetéssel kell biztosítania, hogy az alkalmazottak felkészültek legyenek az új kihívásokra. [TRAC A2.3, Nestor 4.2, PLEDGE OEL-0009

2.1.4. A FOLYAMATOK KISZÁMÍTHATÓSÁGA ÉS SZABÁLYOZÁSA (KSZ)

2.1.4.1. A levéltárnak az elektronikus iratok megőrzésének meghatározó területein rendelkeznie kell szabályzatokkal és dokumentált eljárásrenddel. (KSZ_SZAB)

A levéltár szabályzatai, eljárásrendjei, a munkatársak feladat- és hatáskörei és eljárásai legyenek teljes körűek az elektronikus iratok tekintetében is. A dokumentumok legyenek naprakészek és szabályozott, rendszeres felülvizsgálaton keresztül érvényesítsék az elektronikus levéltár növekedéséből, a technológia illetve a levéltárhasználók elvárásainak és gyakorlatának változásaiból következő módosításokat. Szükséges szabályozni a dokumentumok felülvizsgálati ciklusát, a dokumentumok felülvizsgálatával kapcsolatos eljárást és a frissítési és kiegészítési mechanizmusokat.

Az elektronikus archiválás során a folyamatok maguk is adattá válnak, ezért elengedhetetlen, hogy a szabályzatok pontos előírásokat tartalmazzanak az elektronikus iratok megőrzésének meghatározó területein, mint például az iratátvételi követelmények, az iratok tartalmi és formai ellenőrzése, tárolás, katasztrófatervezés, metaadat-kezelés, kutatás, jogosultságkezelés, megőrzési stratégiák, munkatársak, feladatkörök, biztonság. A szabályzatoknak magas szinten ki kell fejezniük a a szervezet kötelezettségvállalásait és céljait. Az alacsonyabb szintű szabályoknak egyértelműen átláthatóvá kell tenniük a működési gyakorlatot és folyamatokat.

A levéltárnak szabályzatokkal kell rendelkeznie, vagy létező szabályzatait az elektronikus iratok vonatkozásában ki kell egészítenie a következő területeken:

- Ügyrend SZERV_STRUKT, SZERV_SZEREP, SZERV_SZETV, ADATK_MAROGZITES;
- Gyűjtőterületi politika SZK_KIV;
- Iratátvételi szabályzat BEF_DIGIOBJ, BEF_TELJELL, , BEF_VISSZAIG;
- Archiválási szabályzat BEF_SIPAIP, BEF_AIPAZON, BEF_AIPELLENORZES, BEF_ADMINFMETAADAT, MOT_MEGORZSTRAT, ADATK_MAKOZZETETEL, ADATK_MAROGZITES, HASZN_MASOLAT,

- Kutatótermi szabályzat HASZN_KUTSZAB, HASZN_HOZZAFBIZT, HASZN_JOGOSULTSAG, HASZN_OSSZESKERES;
- Információbiztonsági és adatkezelési szabályzat - INFBIZT_IBSZ, INFBIZT_ELL, FIZB_HOZZ, FIZB_BER, AZON_KIKENYSZERIT, AZON_SIKERTELEN, HOZZ_RENDSZFUNKC, HOZZ_SZEREPKOR, MENT_AUTMENT, MENT_INFBIZT, INC_FELISM, INC_KEZ;
- Katasztrófaterv – KAT_KATTERV, KAT_FOLYT

Ezeknek a dokumentumoknak a változatait a levéltárnak megfelelően kell kezelnie, a nyilvános tartalmúakat közzétennie az elavult, hatályon kívül helyezett változatokat egyértelműen megkülönböztetve az érvényesektől. [TRAC A3.2, A5.5, PLEDGE OEL-0012]

2.1.4.2. A levéltárnak teljes körűen dokumentálnia kell az iratok életciklusa során bekövetkező eseményeket, rögzítve az információs csomagokat érintő beavatkozások és adminisztrációs folyamatok metaadatait. (KSZ_ELETCIKLUSDOK)

Az iratok megbízhatóságát az iratok kezelésével kapcsolatos folyamatok nyomon követésével, az egyes beavatkozások és események dokumentálásával lehet biztosítani. Ezeket az adatokat az egyes folyamatokkal és beavatkozásokkal egyidejűleg, és azokkal a beavatkozásokkal, amelyre vonatkoznak összefüggésben kell létrehozni. Az adatok létrejöhetnek automatikus módon vagy rögzíthetők emberi beavatkozás segítségével, az általuk leírt tevékenység természetétől függően.

- Az iratok átvételének előkészítése során (BEF_ELOK)
- A SIP-ek érkeztetésekor (BEF_TELJELL)
- A SIP-ek ellenőrzésekor (BEF_TELJELL)
- A SIP-ek befogadásakor (BEF_BEAV).
- Az AIP készítése során (BEF_AIPAZON) (BEF_AIPELLENORZES) (BEF_ADMINFMETAADAT)
- Az AIP-AIP konverzió során (FELD_BEAVROGZ)
- Az információs csomagok selejtezésekor (FELD_SEL)

2.1.4.3. A levéltárnak rendelkeznie kell a digitális tartalom megőrzéséhez és kezeléshez szükséges jogi felhatalmazásokkal. (KSZ_FELH)

Mivel a digitális információ megváltoztatásának vagy módosításának joga gyakran törvényben szabályozottan a tulajdonoshoz kötődik, fontos, hogy a levéltárak képesek legyenek az elektronikus iratokon tekintetében állományvédelmi célú változtatásokat végezni az értelmezhetőség fenntartása érdekében. Magániratok esetében a letét, ajándékozás és vásárlás lehetővé teszi, hogy az iratok átadója korlátozásokat határozzon meg az iratok levéltári őrzésére illetve az állományvédelmi beavatkozásokra vonatkozóan (10/2002. 18.§ (1)) Hasonló a helyzet az ideiglene-

sen a levéltárba került levéltári anyaggal kapcsolatban. (10/2002. 42.§) Azokban az esetekben, amikor az elektronikus levéltárnak nincs kifejezett jogszabályi felhatalmazása az elektronikus iratokon változást eredményező állományvédelmi beavatkozásokra, az iratátadókkal írásba foglalt megállapodásokon keresztül kell meghatározni és/vagy átruházni ezeket a jogokat a levéltárra.

Szükség esetén a levéltárnak be kell mutatnia azokat a megállapodásokat, amelyek lehetővé teszik a magániratokon végrehajtott állományvédelmi beavatkozásokat. [TRAC A3.3, PLEDGE CU-0006]

-14-

2.1.4.4. Az elektronikus levéltárnak átláthatónak kell lennie minden olyan tevékenységét illetően, ami az elektronikus levéltár működését és irányítását érinti. Különös tekintettel azokra, amelyek a digitális tartalom hosszútávú megőrzésére is hatással vannak. (KSZ_ATL)

Az átláthatóság a legmegfelelőbb bizonyítéka annak, hogy az elektronikus levéltár a releváns szabványokkal és elfogadott szabályzatokkal összhangban működik. Az átláthatóság elengedhetetlen a levéltár megbízhatóságának megteremtéséhez. Az elektronikus levéltár tegyen az érdekeltek számára elérhetővé és hozzáférhetővé minden információt működéséről, teljesítményéről és fejlesztéseiről. A levéltárnak közérdekű adatként közzé kell tennie szervezeti felépítését, a tevékenységére és működésére vonatkozó adatokat, a gazdálkodására vonatkozó közérdekű adatokat. A szokásos kommunikációs csatornák melyeket a fontos hírek és újdonságok közzétételére használnak, elegendő ennek a követelménynek a tejesítéséhez. [TRAC A3.7, RPJ. 2.3.3, PLEDGE OEL-0016]

2.1.4.5. A levéltár határozza meg az általa tárolt információ integritás-ellenőrzésének módszereit, az ellenőrzések eredményét gyűjtse össze, és igény szerint tegye hozzáférhetővé. (KSZ_INT)

A levéltárnak ki kell fejlesztenie vagy alkalmaznia kell megfelelő méréseket az elektronikus levéltári anyag integritásának ellenőrzésére.

Az integritásmérés mechanizmusa a technológia fejlődésével együtt fejlődik, de jelenleg is vannak rá megoldások, mint pl. ellenőrzőösszeg képzése a befogadáskor vagy feldolgozáskor. A megőrzési lánc valamennyi információs csomag esetében a beadás pillanatától kezdve nyilvánvaló, teljes, pontos és időszerű kell legyen. Az elektronikus levéltárnak demonstrálnia kell, hogy az archívumban őrzött tartalom megfelel a megkapott tartalomnak. Erre megfelel egy olyan nyilvántartási funkció, amely dokumentálja az egyes információs csomagok életciklusát a beadástól kezdődően.

Szükséges az archívum integritásmérésének meghatározása, az integritásmérés folyamatainak és mechanizmusának dokumentációja, ellenőrző rendszer az integritás-mérések eredményének összegyűjtésére, nyomon követésére és megjelenítésére, az elektronikus tartalomra kockázatokat jelző integritásmérések eredményére reagáló folyamatok leírása és megvalósítása. A konverzióval és más állományvédelmi beavatkozásokkal kapcsolatos veszteségeket szintén dokumentálni kell és hozzáférhetővé tenni a megfelelő érdekeltek számára.

Az integritás-ellenőrzés lehet egy alkalmazás által a háttérben zajló ütemezett fájlhiba és konzisztencia ellenőrzés (pl. Fedora, Safety Deposit Box), amely megvizsgálja, hogy minden, a levéltári nyilvántartás számára ismert tartalmi fájl valóban jelen van a tárolórendszerben és megfelel a hozzá tartozó checksumnak. Néhány tárolórendszer önmagában is képes ellenőrizni a fájlhibát, a nyilvántartó adatbázis konzisztencia ellenőrzése azonban így is fontos, mert biztosítja, hogy valamennyi fájl ténylegesen létezik és így az adatbázis és a tárolórendszer összhangban van.

[TRAC A3.8, C1.5, C1.6., PLEDGE PP-0016]

2.1.4.6. A levéltár szerződésekből fakadó kötelezettségei legyenek egyértelműek. (KSZ_SZERZ)

Valamennyi kötelezettséget egyértelműen és számon kérhető módon kell meghatározni, körülhatárolt szerepekkel, felelősségekkel, időkeretekkel és feltételekkel, az érdekeltek számára hozzáférhetően vagy hozzáférésre kész módon. A szerződésekbe beleértendők a letéti szerződések, csakúgy, mint azok a szerződések, amelyek az elektronikus levéltár és a számára szolgáltatást nyújtók (rendszerszolgáltatási, karbantartási szerződések), rendszerfejlesztők, stb. között jöttek létre.

2.1.4.7. Az elektronikus levéltár tartsa nyilván a levéltári anyaggal kapcsolatos szerzői jogokat. (KSZ_SZERZOIJOG)

Az elektronikus levéltár tartsa nyilván az iratokkal együtt átvett és ily módon rendelkezésre álló metaadatokat a szerzői joggal érintett iratokról. A nyilvántartásban szereplő korlátozásokat érvényesítse az elektronikus levéltár tartalmának használata során. [TRAC A5.4, PLEDGE PP-0009]]

2.1.4.8. Az elektronikus levéltár dokumentálja a működésével, folyamataival, szoftver és hardver elemeivel kapcsolatos változtatásokat. Ahol szükséges, ezt kapcsolja hozzá a megfelelő megőrzési stratégiákhoz és fogalmazza meg ezeknek a levéltári anyagra gyakorolt potenciális hatását. (KSZ_VALTKOV)

Az elektronikus levéltárnak teljes körűen dokumentálnia kell a bekövetkezett változtatásokat és fejlesztéseket, beleértve az intézményi és technológiai infrastruktúrával kapcsolatos döntéseket. Különös figyelemmel kell rögzíteni az elektronikus levéltárra egészére hatást gyakorló változta-

tásokat és az információs csomagokon, azok halmazain, vagy az információs csomag szintű metaadatokban és a megőrzési stratégiák során alkalmazott eljárásokban bekövetkező változtatásokat. Amennyiben a levéltár szoftvert használ ezek dokumentálására, a szoftvernek képesnek kell lennie a változások nyomon követésére is. [TRAC A3.6, PLEDGE PP-0007]

2.1.5. FENNTARTHATÓSÁG (FENNT)

2.1.5.1. A levéltárnak a fenntarthatóságot a finanszírozás tervezésével is biztosítania kell. (FENNT_FIN)

Viszonylag kevés gyakorlati tapasztalat van arról, hogy az elektronikus iratok hosszú távú megőrzése milyen költségekkel jár, és arról is ellentmondóak a vélemények, hogy a hagyományos iratok vagy az elektronikus iratok megőrzése a költségesebb. Az azonban mindenképp elmondható, hogy az elektronikus iratok megőrzésének költségtényezői jelentősen különböznek a hagyományos iratokétól és folyamatos tervezést igényelnek. Szintén elmondható, hogy a költségek jelentősen függnek a választott megőrzési stratégiáktól.

Az elektronikus iratok értelmezhetőségének fenntartása érdekében folyamatosan biztosítania kell az alkalmazott technológia korszerűsítését, ezért az elektronikus levéltár megbízhatóságára a pénzügyi instabilitás közvetlen hatással van. Valamennyi elektronikus levéltárnak terveznie kell az elektronikus levéltári feladatok finanszírozását, amelyet évenként felül kell vizsgálnia. Mind az elektronikus levéltári funkció létrehozására, mind pedig a már működő elektronikus levéltár beruházásaira vonatkozóan gazdaságossági számításokat kell végezni és biztosítani kell a fenntarthatóság pénzügyi fedezetét.

Az elektronikus iratok megőrzését számos költségtényező befolyásolja. Ezek közül a következők a meghatározók:

A választott és alkalmazott megőrzési stratégiák

Az egyes iratok megőrzési stratégiájának ugyancsak része a gazdaságossági számítás. A megőrzés olcsóbb módjai hatással lehetnek az iratok minőségére, teljességére. Nyilvánvaló az is, hogy nem érdemes hatalmas ráfordításokkal komplex multimédia objektumok teljes körű megőrzését biztosítani, ha azt a levéltárhasználók nem kutatják. A teljesebb metaadatok a megőrzés nagyobb biztonságát nyújtják, de előállításuk költsége tetemes lehet.

A megőrzési stratégiáknak arányban kell lenniük a fenntartott tulajdonságok értékével. Természetesen a gyorsan változó technológiai lehetőségek jelentősen befolyásolják ezeket a döntéseket, ezért az egyes információs csomagokra alkalmazott megőrzési terveket ennek tükrében felül kell vizsgálni.

A megőrzendő tulajdonságok

Az elektronikus iratok valamennyi tulajdonságának teljes körű megőrzése nem minden esetben indokolt. A szöveges dokumentumok jelentős részét csak a szövegben lévő jelentés miatt szükséges megőrizni, miközben a dokumentum metaadatainak, a dokumentumhoz kötődő hitelesítéseknek, a dokumentum viselkedésében rejlő információnak, a beágyazott linkeknek a megőrzése mérlegelhető. Több, összetettebb tulajdonság megőrzése magasabb költséggel jár a megőrzés és a megjelenítés során is.

A használatra bocsátás színvonala

Az elektronikus iratok megőrzésének költségeihez hozzátartozik, hogy az archívumban őrzött bitekből a levéltárhasználók számára értelmezhető információt kell megjeleníteni. A megőrzés nem szükségszerűen jelenti azt, hogy azok felhasználásra kész állapotban vannak. A használatra bocsátás színvonala, a kínált szolgáltatások sokfélesége közvetlenül hat a megőrzés költségeire.

Adattípusok és formátumok sokfélesége

A megőrizni kívánt adatok sokfélesége közvetlenül növeli a költségeket, mivel az egyes információs objektum típusok (adatbázisok, táblázatok, mozgóképi és hangállományok, interaktív multimédia állományok, térinformatikai rendszerek stb.) megőrzése különböző eszközöket igényel. Egy adott információs objektumhoz is több fájlformátum tartozhat így például képi állományok GIF, TIFF, JPEG, PNG etc. Nyilvánvalóan, minél nagyobb ezek sokfélesége, annál több feladatot jelent a megőrzésük, ami növeli a költségeket is. (Cost 2000. 2-5.o.)

A felmerülő költségeket a leginkább gyakorlatias megközelítéssel a Holland Nemzeti Levéltár költségmodellje (Cost 2005) tartalmazza. Ez a következő tételekkel számol:

1. Az elektronikus levéltári anyag megőrzésével kapcsolatos dologi költségek.
    1.1 Létesítménnyel és létesítményüzemeltetéssel kapcsolatos költségek
        1.1.1 Géptermek
        1.1.2 Irodák
        1.1.3 Tárgyalóterem
        1.1.4 Kiszolgáló helyiségek
        1.1.5 Biztonság
    1.2 Az elektronikus levéltár hardvereszközei
        1.2.1 Szerverek

1.5.3 Biztonsági szoftverek

1.5.4 Régi alkalmazások

1.5.5 Fejlesztéshez szükséges alkalmazások

1.5.6 Állományvédelemhez szükséges alkalmazások

1.5.7 Teszt és ellenőrző alkalmazások

1.5.8 Kommunikációs alkalmazások

1.5.9 Adatbázislicenszek

2. Személyi költségek

3. Az állományvédelmi beavatkozásokhoz szükséges módszertan és szoftverfejlesztéssel kapcsolatos költségek.

4. Az állományvédelmi beavatkozások végrehajtásához szükséges költségek

5. A használatra bocsátáshoz szükséges költségek

[TRAC 4.1, 4.2, 4.3, 4.4, 4.5, Nestor 4.1, PLEDGE OEL-0003, PLEDGE OEL-0006]

2.1.5.2. A levéltár kérje, fogadja és kezelje az iratképzők és felhasználók részéről a levéltári szolgáltatással kapcsolatos visszajelzéseket (FENNT_VISSZAJ).

Az elektronikus levéltárnak szisztematikusan és rutinszerűen törekednie kell arra, hogy visszajelzésekhez jusson a szolgáltatásával kapcsolatba kerülő érdekeltektől. Ezek a visszajelzések teszik lehetővé, hogy az elektronikus levéltár figyelemmel kísérhesse, hogy szolgáltatása során megfelel-e a technológiai fejlődés és a felhasználói igények által támasztott követelményeknek. A követelmény teljesítése támogatható olyan automatikus eljárásokkal, amelyek visszacsatolási mechanizmusokat tartalmaznak, eljárásokkal, amelyek a visszacsatolás eredményeinek feldolgozását, fogadását és dokumentálását célozzák, és támogatják a visszacsatolási munkafolyamat dokumentálását [TRAC A3.5, PLEDGE OEL-0015]

2.1.5.3. A levéltárnak az elektronikus iratok megőrzésével kapcsolatos tevékenységét rendszeres felülvizsgálatnak és értékelésnek kell alávetnie annak érdekében, hogy képes legyen tartani a lépést a technológia fejlődésével és a változó követelményekkel. (FENNT_ERT)

A hosszú távú megőrzés összetett feladat, a nemzetközi levéltári közösség közös felelőssége. Egy megbízható elektronikus levéltár hozzájárul a közösség módszertani eredményeihez és felhasználja mások eredményeit. A hazai és nemzetközi gyakorlat alapján történő rendszeres felülvizsgálat szükséges eleme az elektronikus levéltár folyamatos és hatékony fejlődésének.

Számos projekt és megvalósítás célozza meg az elektronikus iratok megőrzésének különböző aspektusait. A legteljesebb keresést az Ausztrál Nemzeti Levéltár PADI szolgáltatása (http://www.nla.gov.au/padi/) biztosítja, az alábbiakban csak a legfontosabb szereplőket és eredményeket említjük meg a közlevéltárak további tájékozódását segítendő.

Kutatási projektek

- Digital Preservation Europe – az ERPANET projekt folytatásaként alakult, fontos termékei a PLATTER útmutató az elektronikus levéltárak tervezését segíti, és a DRAMBORA, ami a kockázat alapú auditálási segédlet. http://www.digitalpreservationeurope.eu/
- PLANETS – Nemzeti könyvtárak, levéltárak, egyetemi kutatóintézetek és magáncégek részvételével 2006-ban indult és 2010-ben lezáruló projekt. Hasznos terméke a PLATO megőrzéstervező eszköz és a PLANETS testbed, az állományvédelmi szoftverek közösségi tesztelését szolgáló felület. http://www.planets-project.eu/
- CASPAR – Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval. Az EU 6. keretprogramjából 2006-2009 között finanszírozott projekt több prototípus terméket hozott létre és hasznos képzési anyagok érhetők el a honlapján. http://www.casparpreserves.eu/caspar-project
- InterPares3 - International Research on Permanent Authentic Records in Electronic Systems. A University of British Columbia által koordinált projekt a két előző projektfázis tapasztalatait kívánja a gyakorlatba átültetni. Az egész világra kiterjedő tevékenysége főleg az oktatást célozza meg. http://www.interpares.org/ip3/ip3_index.cfm

Nemzeti közgyűjteményi együttműködések

- Digital Preservation Coalition. 2001-ben alakult közösség az Egyesült Királyságban a digitális megőrzésben érdekelt szervezetek együttműködése. http://www.dpconline.org/
- nestor Project 2003-2009 között a Német Oktatási és Kutatási Minisztérium által finanszírozott projekt kutatási intézetek, könyvtárak és levéltárak részvételével. Számos szabványt és útmutatót készített, a közelmúltban jelent meg a projekt tapasztalatait összegző átfogó kiadvány. http://www.langzeitarchivierung.de/eng/ueber_uns/index.htm

Megvalósult megoldások

- DIMAG – Baden-Württenberg levéltári projektje 2006-ban indult és nagy diverzitású jelentős iratanyagot vettek át az azóta eltelt időben. Meghatározóan open-source termékekre alapozva metaadatszabvány-szkeptikus minimalista megközelítés. (Handbuch Kap.11.7-8., http://www.ijdc.net/index.php/ijdc/article/view/120/0)

- PANDORA – Az Ausztrál Nemzeti Könyvtár által 1996-ban indított webarchívum, amely kilenc további intézménnyel együttműködve online publikációkat archivál. Fontos ismérve a valós megjelenésű „look-and-feel" archiválás. http://pandora.nla.gov.au/about.html
- FEDORA – A Cornell University és a University of Virginia könyvtárának együttműködésében készült elektronikus archiváló alkalmazás, nyilvántartó és ingest funkcióval, integráltan a JHOVE és DROID alkalmazásokkal. http://www.fedora-commons.org/
- KOPAL – A Német Szövetségi Könyvtár, a göttingeni egyetem és az IBM közös projektje a DIAS szoftver németországi alkalmazására. A projekt kifejlesztette az opensouce KoLibRi szoftvert információs csomagok létrehozására, importálására és lekérdezésére. A szoftver előnye a konfigurálható munkafolyamat.
  http://kopal.langzeitarchivierung.de/index_software.php.en
- BAR – A svájci Bundesarchiv OAIS megoldása az Arelda projektre építve kereskedelmi termékek és opensource alkalmazások ötvözésével alakította ki archiválási megoldását. 2009 őszén bocsátotta közre Siard Suite alkalmazását, amely relációs adatbázisok hosszú távú megőrzését támogatja. http://www.bar.admin.ch/index.html?lang=en
- Österreichisches Staatsarchive – A 2006-tól az Osztrák Állami Levéltár és a Szövetségi Kancellária által közösen előkészített PPP projekt beszerzését 2009-ben az angol-amerikai Tessella cég nyerte el. A megvalósítás az Ediakt II e-kormányzati adatcsereszabványt (metaadatok XML-ben, dokumentumok PDF/A-ban. http://www.oesta.gv.at/

[TRAC A3.4]

2.2. Digitális tartalomkezelés

Ez a fejezet az elektronikus levéltári iratok levéltári kezelése során megvalósított beavatkozásokra vonatkozó szabályokat, követelményeket írja le, amelyeken keresztül az elektronikus levéltár biztosítja az iratok hosszú távú értelmezhetőségét.

Az elektronikus levéltár digitális objektumkezeléssel kapcsolatos feladatai természetesen érintik mind a szervezeti, mind a műszaki követelményeket. A digitális objektumkezelés követelményei ugyanakkor előfeltételei az infrastrukturális követelményeknek. A digitális objektumok életciklus-kezeléséhez tartozó követelményeket az elektronikus levéltár funkcionalitásából kiindulva hat csoportba osztottuk, a csoportosításhoz felhasználva a jól ismert OAIS funkcionális egységeket, kiegészítve az iratátvétel és a levéltári feldolgozás funkcióval:

- Az iratátadás előkészítése, iratátvétel (BEF)
- Megőrzéstervezés. (MOT)
- Tárolás, őrzés. (TAR)

- Adatkezelés. (ADATK)
- Levéltári feldolgozás. (FELD)
- Hozzáférés, használat. (HASZN)

Az objektumkezelés követelményei szintén az OAIS modellen, annak információs modelljén alapulnak, amely meghatározza a Befogadott Információs Csomagot (SIP), az Archív Információs Csomagot (AIP) és a Kibocsátott Információs Csomagot (DIP).

Az objektumkezelés általános követelménye és valamennyi művelet során biztosítani kell az objektum integritását és hozzáférhetőségét, a nyomon követhetőséget, a hivatkozási integritás megőrzését.

Az alábbi követelmények feltételezik az OAIS modell ismeretét.

2.2.1. IRATÁTVÉTEL ELŐKÉSZÍTÉSE ÉS IRATÁTVÉTEL (BEF)

Az elektronikus levéltárak folyamatai leginkább a befogadási folyamatok területén különbözhetnek, annak megfelelően, hogy milyen típusú anyagokat vesznek át és az átvétel során milyen a kapcsolatuk az iratképzőkkel. Valamennyi elektronikus levéltárra igaz viszont, hogy a befogadás akkor fejeződik be, amikor az Archív Információs Csomag (AIP) és a hozzá társított metaadatoknak a levéltár rendszereiben való biztonságos elhelyezése megtörténik, beleértve természetesen a szükséges biztonsági másolatok létrehozását is.

A közlevéltárak az illetékességükbe tartozó iratképzőket a levéltári törvény alapján felszólíthatják a köziratok átadására, a magániratok tekintetében azonban ilyen lehetőségük nincs. Az átadás előkészítése során a levéltár az iratképzővel együttműködve megvizsgálja az átadandó iratokat meghatározza az iratképző számára azokat a feladatokat, amelyeket a levéltári átadás feltételeként végre kell hajtania. Az is előfordulhat, hogy az előkészítés során a levéltárra hárulnak feladatok, amennyiben a maradandó értékű anyag fogadására fel kell készülnie. Elektronikus környezetben az is előfordulhat, hogy az iratképző-elektronikus levéltár kapcsolat automatikus.

Az átadást követően az elektronikus levéltár a beadott SIP-et biztonsági, formai és tartalmi ellenőrzésnek veti alá.

Az elektronikus levéltáraknak aktív megőrzési beavatkozásokat kell végrehajtaniuk annak érdekében, hogy megőrizzék a befogadott információt és hogy azok az anyagok, amelyeket a felhasználókhoz eljuttatnak, ha nem is identikusak de „szoros kapcsolatban legyenek” az átadott eredeti objektumokkal. Minden egyes átvett és ellenőrzött információ (az adatobjektumok és a megfelelő metaadatok) nem az eredeti, hanem archív formában kerül tárolásra az elektronikus levéltár tárhelyén. Az elektronikus levéltár ezért az iratátvételi folyamat befejezéseként létrehoz-

za az archív tárolás számára alkalmas és azonosítható formátumot, amelyben az információt ezt követően tárolni fogja. Ennek során rögzíti a szükséges levéltári metaadatokat, elvégzi azok összekapcsolását az elvárt értelmezhetőségi szint szerint, az egyedi azonosítók hozzárendelését az AIP hivatkozásának megteremtéséhez, a SIP összekapcsolását az AIP-pal, a proveniencia információ létrehozását. Mindezt oly módon, hogy biztosítja, hogy az AIP készítés során nem történik veszteség vagy sérülés a tartalomban.

2.2.1.1. A levéltárnak biztosítania kell az iratok életciklus menedzsment szemléletű megközelítését. (BEF_PREV)

Az elektronikus iratok sajátosságaiból adódóan a levéltárak részéről szükséges az iratkezelési folyamat életciklus-menedzsment szemléletű megközelítése. A köziratok tekintetében a levéltárak feladatainak ki kell terjednie a maradandó értékű iratokat kezelő rendszerek tervezésével kapcsolatos tanácsadásra, az iratkezelési szabályzatok jóváhagyásán keresztül az iratkezelési folyamatok működésének, az iratok létrehozásának, kezelésének, tárolásának ellenőrzésére a maradandó értékű iratok tekintetében ellenőrzési joggal.

2.2.1.2. Az elektronikus levéltár egyértelműen határozza meg azokat az információkat, amelyeket a digitális anyaggal együtt át kell adni az átadás során, a digitális objektumok szerkezetét és a beadás lehetséges módjait. (BEF_DIGIOBJ)

A befogadásra kerülő digitális objektumokra vonatkozóan az elektronikus levéltárnak iratátvételi szabályzatában rögzített ismérveket kell meghatároznia. Ezt készítheti maga az elektronikus levéltár, de a köziratok közlevéltárba adása esetében származhat jogszabályból is. Az iratátvételi szabályzatnak pontosan meg kell határoznia, az iratképzőtől/iratátadótól milyen digitális objektumok vehetők át, milyen dokumentációt kell társítani az objektumokkal és minden hozzáférési korlátozásokat kell a használatra bocsátásukkor érvényesíteni. Meg kell határozni, hogy a beadás során mely elfogadott metaadat-szabványokat (pl. METS, XFDU, PREMIS, LMER, EAD, DC, MIX) érvényesít. Ugyancsak meg kell határozni a digitális objektumok szerkezetét és a beadás lehetséges módjait (adathordozó, kommunikációs csatorna). Ezek a paraméterek egyben az ellenőrzés alapját is jelentik. [TRAC B1.2, Nestor 9.1, PLEDGE PP-0011, PLEDGE PP-0018]

2.2.1.3. Az egyes iratátvételek előkészítése során levéltári átadási megállapodásban szükséges részletezni az iratátvétel konkrét módját. (BEF_ELOK)

A levéltár lehetőség szerint szabványosított dokumentumban meghatározza, hogy melyek azok a szempontok, amelyeket az átadandó anyagra érvényesíteni kíván. Ezek a szempontok lehetnek egyediek vagy származhatnak meglévő jogszabályokból és szabványokból. A megállapodás a maradandó értékűként meghatározott iratokat az átvételhez szükséges részletességgel leírja. Meghatározza, hogy az iratok milyen funkciót töltöttek be az iratképzőnél, általános tartalmi leírást és iratértékelést készít, továbbá rögzíti jellemző technikai és logikai paramétereket (iratok

típusa, struktúrája, fájlformátumok, méretek, jogosultságok, szerzői jogok, hitelesség). A leírás során törekedni kell arra, hogy az információ szerkezete igazodjon a levéltári leírás szerkezetéhez. Annak érdekében, hogy a levéltár meghatározza a maradandó értékű iratokat, információkat gyűjt az iratképzőről, tevékenységéről és az átadni kívánt iratokról. A megállapodásnak tartalmaznia kell a segédletekkel ellátottságot, a SIP definíciókat, az átadott anyag terjedelmét, tartalmát és az átadás idejét. A letéti megállapodásnak tartalmaznia kell a tulajdonjogokat, hozzáférési jogokat, a visszaadás feltételeit is. A megállapodást a levéltár és az iratátadó közösen készíti el és az abban foglaltak mindkét félre vonatkozóan betartandók.

Egy példa a követhető szabványra a CCSDS/ISO Producer-Archive Interface Methodology Abstract Standard (PAIMAS).

Az átadás történhet a levéltár telephelyén vagy on-line módon. Az átadás során való azonosításra felhasználható a központi elektronikus szolgáltató rendszer szervezeteket azonosító szolgáltatása (Hivatali Kapu) a 225/2009. (X.14.) Korm. sz. rendelet 29 § szerint.

Az átadási megállapodásnál tekintettel kell lenni a vonatkozó jogszabályokra és azokban rögzített átadási szabályokra és a levéltárnak az átadással kapcsolatos belső szabályozására. [TRAC A5.2, A5.3, A5.5, PLEDGE CU-0006]

2.2.1.4. A közlevéltárnak biztosítania kell a tanúsított iratkezelési szoftvereknek a levéltári átvételi követelményeknek megfelelően kialakított SIP állományainak fogadását. [BEF_ISZ]

Közlevéltár esetében az elektronikus levéltárnak biztosítania kell a 24/2006 4. §-ban leírt Iratkezelési Szoftver export/import interfészen keresztül történő adatátvételt. Amikor az ISZ egy irattári tételszámhoz tartozó iratokat, egy iktatókönyvhöz tartozó iratokat, ügyiratot vagy iratot ad át, annak az alábbiak átadásával kell járnia:

a) (irattári tételszám esetében) a megadott időszakra vonatkozóan a tételszámhoz tartozó összes irat,

b) (iktatókönyvek esetében) az iratokhoz tartozó összes iktatókönyv,

c) (ügyiratok esetében) a hierarchiában az ügyirat alatt elhelyezkedő összes irat,

d) az ilyen iratokhoz társuló valamennyi jogszabályban vagy annak hiányában a levéltári átadásban rögzített metaadatot.

Az iratátadó felelőssége biztosítani, hogy az export során

- nem sérül az elektronikus iratok tartalma és struktúrája,

- az elektronikus irat valamennyi komponense egy szerves egységet képezve kerül exportálásra,
- megőrzi az irat és annak metaadatai közötti kapcsolatot.

Az iratképzőnek biztosítania kell, hogy a levéltárba adás során átadja valamennyi, jogszabályban vagy annak hiányában a levéltári átadási megállapodásban rögzítetteseménynapló adatot.

Az iratképzőnek biztosítania kell, a vegyes iratok együttes levéltári átadását.

[24/2006 4. § , 8.3.1, 8.3.2, 8.3.3]

2.2.1.5. Az elektronikus levéltárnak azonosítási mechanizmussal kell rendelkeznie az anyagok forrásának ellenőrzésére. (BEF_FORRASELL)

Az elektronikus levéltár folyamatainak és tényleges gyakorlatának biztosítania kell, hogy a külső forrásból megszerzett digitális objektumok esetén a megfelelő proveniencia fenntartása megtörtént és hogy az objektumok valóban azok, amelyeket az elektronikus levéltár elvárt. Ennek megerősítése különböző módon történhet: a digitális feldolgozás, adatellenőrzés és validálás során, az iratátvétel tényleges ellenőrzésén és átadás-átvételi jegyzőkönyvön vagy Központi Elektronikus Szolgáltató Rendszer szervezeteket azonosító szolgáltatásán (Hivatali Kapu) keresztül. [TRAC B1.3, PLEDGE PP-0010, 225/2009. (X.14.) Korm. sz. rendelet 29 §]

2.2.1.6. Az elektronikus levéltárnak a befogadási folyamat során ellenőriznie kell minden egyes benyújtott objektumot/SIP-et az átadás során megkövetelt információk teljességének és pontosságának tekintetében. (BEF_TELJELL)

A befogadási folyamat során meg kell valósítani a SIP-ek biztonsági, formai és tartalmi ellenőrzését. A befogadási folyamat során összegyűjtött információt össze kell vetni az iratképző vagy az elektronikus levéltár saját elvárásaival, hogy ellenőrzésre kerüljön az adatátadás és a befogadási folyamat helyessége. Az a tartomány, amelyben az elektronikus levéltár meghatározza a helyességet, attól függ, hogy milyen információkkal rendelkezik a SIP-ről és milyen eszközök állnak rendelkezésére a SIP megfelelőségének ellenőrzésére. Ez jelentheti egyszerűen a fájlformátumok ellenőrzését, illetve, hogy a formátumok valóban azok, amiknek látszanak (például a TIFF fájlok érvényes TIFF formátumban vannak-e), annak automatikus ellenőrzését, hogy a metaadatok ki vannak-e töltve és megfelelnek-e valamilyen szabálynak (pl. a dátum dátum értéket tartalmaz-e), továbbá magában foglalhatja a tartalom ellenőrzését, némely esetben emberi közreműködéssel, mint például annak megállapítása, hogy egy kép leírása valóban a képre vonatkozik-e, vagyis, hogy a metaadatok minősége megfelelő-e.

A formátumok ellenőrzéséhez szükséges információt az elektronikus levéltár kezelheti lokálisan, vagy használhatnak nemzetközi formátum-nyilvántartó adatbázisokat is, mint például a következők.

- File Format Encyclopedia, http://pipin.tmd.ns.ac.yu/extra/fileformat/
- FILExt http://filext.com/
- Library of Congress Digital Formats http://www.digitalpreservation.gov/formats/fdd/browse_list.shtml
- C.E. Codere's File Format site http://magicdb.org/stdfiles.html
- PRONOM http://www.nationalarchives.gov.uk/pronom/
- Global Digital Format Registry http://hul.harvard.edu/gdfr/
- Representation Information Registry Repository, http://registry.dcc.ac.uk/omar
- DCC RI RegRep http://dev.dcc.rl.ac.uk/twiki/bin/view/Main/DCCRegRepV04
- FCLA Data Formats http://www.fcla.edu/digitalArchive/pdfs/recFormats.pdf

(Handbuch. Kap 7.20)

A nemzetközi formátum nyilvántartások alkalmazása nem a helyi formátum nyilvántartások helyett történik, sokkal inkább forrásként szolgál a független, megbízható információellenőrzéshez.

Az elektronikus levéltáraknak rendelkezniük kell eljárásokkal a hibás SIP-ek kezelésére. A hibás SIP következménye lehet az átvétel elutasítása, a feldolgozás felfüggesztése a hiányzó információ beérkezéséig, vagy egyszerű hibajelentés. A teljesség definíciója meg kell, hogy feleljen az elektronikus levéltár tevékenységének. Amennyiben a fájlok nyilvántartását az átvételt megelőző egyeztetések részeként az iratképző átadta, elvárható az átadott fájloknak a nyilvántartással való összevetése.. Bármilyen ellenőrzés is kerül végrehajtásra, összhangban kell lennie azzal, amit a levéltár követelményként megfogalmazott az iratátvételi szabályzatában és az iratátvételi megállapodásban. [TRAC B1.4, B2.6, PLEDGE PP-0011, RPJ 2.3.4]

2.2.1.7. Az elektronikus levéltárnak elegendő fizikai kontrollt kell szereznie a digitális objektumokon annak érdekében, hogy gondoskodjon a megőrzésükről. (BEF_FIZKONTROLL)

Az elektronikus levéltárnak teljes kontrollt kell szereznie a SIP-ekben beadott digitális objektumok felett. Néhány SIP például csak hivatkozásokat tartalmaz digitális objektumokra és ilyen esetekben az elektronikus levéltárnak meg kell kapnia a hivatkozott digitális objektumokat, amennyiben azok részét alkotják annak az objektumnak, amelyek megőrzését az elektronikus levéltár vállalta. A kontroll azt is magában foglalja, hogy az elektronikus levéltár hozzá tudjon férni a digitális objektumok tartalmához. Az átvétel során biztosítani kell, hogy ne kerüljön átvételre olyan tartalom, amely kódolás, titkosítás vagy jelszavas védelmen keresztül a tartalomhoz való hozzáférést megakadályozza. A tartalomban ne legyenek olyan beállítások, amelyek megakadályozzák a másolást, nyomtatást vagy bizonyos idő elteltével a tartalmat hozzáférhetetlenné teszik. [TRAC B1.5, Nestor 9.3]

2.2.1.8. *Az elektronikus levéltárnak a befogadási folyamat előre meghatározott pontjain megfelelő visszajelzésekkel kell szolgálni az iratképző/iratátadó számára. (BEF_VISSZAIG)*

Az elektronikus levéltárnak az iratátvételi szabályzatot valamint az iratképző/iratátadó és az elektronikus levéltár között létrejött megállapodást alapul véve, a befogadási folyamat konkrét, előre meghatározott pontjain értesítéseket kell küldenie az iratképző/iratátadó számára. Az elektronikus levéltár értesítései magukban foglalhatják az adatátvitel, az ellenőrzés bizonylatait vagy bizonylatot arról, hogy az AIP létrejött és tárolásra került. Az elektronikus levéltár értesítései terjedhetnek a teljesség és helyesség előre meghatározott rendszeres jelentéseitől, hibajelentésekig vagy bármely végleges átadás-átvételi dokumentumig. Az iratátadók egyedileg kérhetnek a szokásos értesítéseken felül további információkat is, amennyiben a szabályzatban vagy megállapodásban rögzített értesítések elégtelennek bizonyulnak. [TRAC B1.6]

2.2.1.9. *A levéltár visszajelzést küld, amikor a megőrzési felelősséget hivatalosan átveszi a benyújtott SIP-ek tartalmára vonatkozóan, ezzel egyidejűleg nyilvántartásaiban rögzíti az iratok átvételét (BEF_SIPBEF).*

A levéltár az ellenőrzésen átesett SIP-et a gyarapodási naplóba bevezeti. Ennél a pontnál a levéltár hivatalosan átveszi a digitális objektumok megőrzési felelősségét az iratátadótól, amiről az iratátadót átadás-átvételi jegyzőkönyv formájában értesítenie kell. A levéltár számára a digitális objektumok feletti kontroll ugyanakkor csak az iratok archiválásra alkalmas változata, az AIP, létrejöttekor válik teljessé. Ezért a levéltár törzskönyvébe az AIP kerül bevezetésre. [TRAC B1.7, PLEDGE PP-0001]

2.2.1.10. *A levéltár az átvétellel egyidejűleg rögzítse az átvétel során megvalósított beavatkozások adatait (BEF_BEAV).*

Ezeket az adatokat azokkal a beavatkozásokkal egyidejűleg kell rögzíteni, amelyekre vonatkoznak, és amelyekhez kapcsolódnak. Az adatrögzítés lehet automatizált vagy végezhetik a levéltár munkatársai, a megőrzési beavatkozások természetétől függően. [TRAC B1.8, PLEDGE PP-0007]

2.2.1.11. *A levéltár rendelkezzen a hosszú távú megőrzés követelményeinek megfelelő definícióval az archívumban őrzött minden egyes AIP-ra vagy AIP típusra vonatkozóan. (BEF_AIPDEF)*

Egy AIP a következő összetevőket tartalmazza: a megőrzendő elsődleges adatobjektumot, a rá vonatkozó értelmezési információt (formátumot és a formátum-elemek jelentését), a megőrzési információ (PDI) különböző kategóriáit, amelyeket szintén kapcsolni kell az elsődleges adatobjektumhoz: így a változatlansági, proveniencia, kontextuális és hivatkozási információkat. Szükséges azt is definiálni, hogy ezek a metaadatok hogyan kapcsolódnak egymáshoz, hogy mindig megtalálhatóak és kezelhetők legyenek a levéltárban, és hogy a metaadatokra vonatkozóan a levéltár milyen szabványokat (METS, XFDU, PREMIS, LMER, EAD, DC, MIX) érvényesít

Követelmény, hogy minden egyes AIP-hoz, vagy amennyiben több hasonló van, minden egyes AIP típushoz, legyenek definíciók. A levéltárnak, amennyiben amelyek az objektumtípusok széles skáláját tárolják, szükségük lehet az általuk tárolt valamennyi AIP egyedi definiálására, de valószínűleg a legtöbb levéltár létrehoz olyan leírási típusokat, amelyek több AIP-ra is alkalmazhatók. Ebben az esetben azt valószínűleg meg kell határozni, hogy melyik definíció melyik AIP-ra alkalmazható.

A definíciók puszta létezésén túlmenő követelmény, hogy alkalmasak legyenek a hosszú távú megőrzésre, vagyis, hogy mondjon valamit az AIP szándékolt használatáról, amennyiben az a hosszú távú megőrzéssel kapcsolatos döntést befolyásolja.

A nyílt, veszteségmentes és elterjedt formátumok archiválásra inkább alkalmasabbak, hiszen várhatóan hosszabb az élettartamuk, és emellett valószínűsíthetően több eszköz támogatja a használatukat (konverziójukat, emulációjukat), hiszen szélesebb felhasználói kör használja őket. Az archív formátumok kiválasztásánál azonban meg kell teremteni az egyensúlyt az adatok értéke és a tárolás optimalizálása között, különösen, amikor a veszteségmentes formátumok használatára is felmerül (a formátumok kiválasztásának gazdasági szempontjaira ld. SZK_FIN). [TRAC B2.1, B2.2, Nestor 10.1, PLEDGE PP-0002]

2.2.1.12. A levéltárnak leírással kell rendelkeznie arról, hogy a SIP-ből hogyan jön létre az AIP. (BEF_SIPAIP)

Az archiválási szabályzatnak rögzítenie kell, hogy a megőrzött objektum miként jött létre az átvétel során benyújtott objektumból.

Néhány esetben az AIP és a SIP a csomagolástól eltekintve azonos lehet, azonban gyakoribb, hogy az adatobjektumok összetett transzformációkon (pl. adatnormalizáláson) esnek át a befogadási folyamat során. Szükség lehet ezeknek a beavatkozásoknak (pl. metaadatok megőrzése) a pontos leírására annak biztosítása érdekében, hogy az archivált objektum képes legyen reprezentálni az átvett objektumban lévő információt. Az AIP létrehozás leírásának tartalmaznia kell adatokat minden egyes SIP-AIP transzformáció esetében, rögzítve a befogadási folyamat során bekövetkezett SIP-AIP leszármazási kapcsolatot és az AIP-nak a levéltári hierarchiában való elhelyezését vagyis a törzskönyvezést.

Az AIP létrehozás általános feldolgozási folyamat, amely minden egyes ilyen transzformáció esetén alkalmazásra kerül, kiegészítve az ilyen feldolgozások különböző típusainak leírásával és – egyes esetekben – a szükséges különleges transzformációkkal. A beavatkozásokat naplózni kell minden egyes AIP létrehozásakor. Több folyamat esetén egyértelműnek kell lennie,

hogy melyik folyamat mikor, melyik AIP-re (AIP típusra) kerül alkalmazásra. [TRAC B2.3, Nestor 10.3, PLEDGE PP-0002]

2.2.1.13. A levéltárnak demonstrálnia kell, hogy valamennyi benyújtott objektum (SIP) vagy egy végleges AIP-ként archiválásra vagy naplózott módon eltávolításra került. (BEF_SIPALLAPOT)

Az átvételi folyamat a szükséges ellenőrzések és kiegészítések miatt elhúzódhat, de a SIP-eknek nem szabad örökre várakozó állapotban maradnia. Az átvételi eljárásoknak, a belső folyamatoknak és a naplóállományoknak meg kell tartaniuk a SIP valamennyi belső transzformációját, hogy kimutatható legyen, hogy azokból részben vagy egészben AIP-ok készültek vagy nem kerültek befogadásra és az archívumból eltávolításra kerültek. Megfelelő leíró információnak kell dokumentálnia valamennyi digitális objektum leszármazását. Amennyiben a SIP az AIP-on belül tárolásra kerül ez a leíró információ az AIP-on belül található. [TRAC B2.4, PLEDGE PP-0016]

2.2.1.14. A levéltár állandó, egyedi azonosítót generál minden egyes AIP számára. (BEF_AIPAZON)

A levéltárnak szükséges biztosítania, hogy egy elfogadott, irányadó elnevezési konvenciót alkalmaz, amely egyedileg azonosítja az anyagokat és állandó azonosító (persistent identifier, PID) mind a levéltáron belüli, mind a külső használathoz.

Ezzel egyenértékű fontosságú, hogy az egyedileg elnevezett objektum megtalálható legyen a fizikai elhelyezéstől függetlenül. Az AIP-hez kapcsolódó akciók az idők során, a rendszer változásain és a tárolási megoldások változásain keresztül nyomon követhetők legyenek. Ideális esetben az egyedi azonosító mindaddig létezik ameddig az AIP, amennyiben mégsem, nyomon követhető kell, hogy legyen. Az ID rendszernek nyilvánvalóan illeszkednie kell a levéltár jelenlegi és előre látható jövőbeni követelményeihez, mint például a párhuzamosan őrzött papír alapú iratok törzsszáma és jelzete vagy az objektumok esetleg exponenciálisan növekvő száma. Az azonosító egyedisége ellenőrizhető kell, hogy legyen. Az azonosítási követelmények nem korlátozzák az AIP-ok és az egyes fájlok kapcsolatát. Általában egy AIP egy vagy több fájlt foglal magában de az is előfordulhat, hogy egy egyedi fájl tartalmazhat egynél több AIP-ot. Ebből következően az azonosítók és a fájlnevek nem szükségszerűen felelnek meg egymásnak.

Az archiválási szabályzatnak tartalmaznia kell, hogy az AIP állandó azonosítói és annak összetevői hogyan vannak kiosztva és karbantartva, hogy levéltáron belül egyediek maradjanak. [TRAC B2.5]

2.2.1.15. A levéltár rögzíti/nyilvántartja az értelmezési információt (RI) (a formátumokat is beleértve) amelyet befogadott. (BEF_ERTINF)

Abban az esetben, ha a kapcsolódó értelmezési információhoz (RI) nem áll rendelkezésre nemzetközi szabvány, a levéltárnak rögzítenie és nyilvántartásba kell vennie ezeket az információkat, hogy meg lehessen találni és újra fel lehessen használni ezeket. Ezek közül néhányat szoftverbe lehet foglalni. Az értelmezési információ (RI) kulcsfontosságú a bitsorozat használható információvá alakíthatósága szempontjából, ezért a tartalmi információval (CI) való kapcsolatát létre kell hozni és fenn kell tartani. [TRAC B2.8, PLEDGE PP-0014]

2.2.1.16. A levéltár megőrzi a megőrzési metaadatokat (PDI) a kapcsolódó tartalmi információkhoz (CI). (BEF_PDI)

A megőrzési metaadatok (PDI) nem csak a levéltár számára szükségesek, biztosítják a tartalmi információ érintetlenségét, fellelhetőségét, értelmezhetőségét, provenienciáját, kontextusát. Az effajta információs szükséglet mértékét leginkább a levéltárhasználók igényei határozzák meg. A megőrzési metaadatokat (PDI) folyamatosan a tartalmi információhoz (CI) kell kapcsolni és a kapcsolatot fenn kell tartani. [TRAC B2.9]

2.2.1.17. A levéltár rendelkezzen dokumentált folyamatokkal az információs tartalom értelmezhetőségének tesztelésére, és az információs tartalom érthetőségi szintre hozására. (BEF_ERTELMEZ)

Ha a tartalmi információt (CI) vagy megőrzési leírási információt (PDI) a levéltárhasználók által jellemzően használt eszközök nem közvetlenül használják, a levéltárnak rendelkeznie kell egy konkrét folyamattal ezek használható formába való konverziójához vagy további értelmezési információval való ellátásához. [TRAC B2.10, PLEDGE PP-0003]

2.2.1.18. A levéltár a létrehozást követően ellenőriz minden egyes AIP-ot. (BEF_AIPELLENORZES)

Az archiválási szabályzatnak tartalmaznia kell, hogy az adott levéltár az iratátvételi folyamat végén hogyan ellenőrzi a létrehozott AIP-ok teljességét és helyességét formai és tartalmi szempontból. Amennyiben a levéltár rendelkezik standard folyamatokkal a SIP-ek teljességének és/vagy helyességének formai és tartalmi ellenőrzésére, és egy bizonyíthatóan megfelelő eljárással a SIP-ek AIP-okká történő átalakítására, abban az esetben csak annyit kell garantálnia, hogy a kezdeti ellenőrzéseket sikeresen végrehajtotta és az átalakítási folyamat hiba nélkül lezajlik. Azok a levéltárak, melyek egyedi folyamatokat készítenek az AIP-ok létrehozásához, ugyancsak egyedi módszereket kell létrehozzanak az AIP-ok teljességének és helyességének validálására. Ez jelentheti meghatározott tesztek végrehajtását az AIP tartalmára vonatkozóan, amelyek eredményét össze lehet vetni a SIP-eken végzett tesztek eredményével, magában foglalhatja az ellenőrző összegek alkalmazását, az ellenőrző összegek helyességének ellenőrzé-

sét, a véghezvitt ellenőrzések naplózását, és valamennyi speciális tesztet amelyeket az egyes SÍP/AIP-ok vagy SIP/AIP típusok tesznek szükségessé. [TRAC B2.11]

2.2.1.19. A levéltár biztosítsa az általa őrzött elektronikus levéltári anyag egészének integritását. (BEF_INTEGR)

A levéltárnak be kell tudnia mutatni a gyarapodási naplóban rögzített minden egyes levéltári anyagról, hogy a feldolgozás során melyik AIP-ba került. (Spezifikazion SIP) [TRAC B2.12, PLEDGE PP-0016]

2.2.1.20. A levéltár rögzítse az AIP készítés során végrehajtott beavatkozások és adminisztrációs folyamatok metaadatait. (BEF_ADMINFMETAADAT)

Ezeket az adatokat az AIP létrehozással kapcsolatos tevékenységekkel egyidejűleg kell létrehozni. Az adatok létrejöhetnek automatikus módon vagy rögzíthetők emberi beavatkozás segítségével, az általuk leírt tevékenység természetétől függően.

2.2.2. MEGŐRZÉSTERVEZÉS (MOT)

A levéltárnak vagy levéltári rendszernek korszerű, jól működő és dokumentált megőrzési stratégiával kell rendelkeznie. Nem elegendő csupán az információt megőrizni, a levéltár a megőrzést, előre definiált, dokumentált megőrzési szabályok és eljárások szerint kell, hogy végezze. Ezen felül rendszeres tevékenységeként ezeket a megőrzési szabályzatokat és eljárásokat folyamatosan a technológiaváltásokhoz kell igazítania. Nyilvánvalóan nem elvárható, hogy a levéltár megoldással rendelkezzen olyan fájlformátumok megőrzésére, amelyek még nem is léteznek, de kell, hogy legyen stratégiája arra vonatkozóan, hogy mit kell tenni abban az esetben mikor először jelenik meg ilyen ismeretlen fájlformátumú objektum. A levéltár stratégiája lehet, hogy elutasítja az objektumot vagy megvizsgálja a kezelés lehetőségét, de a döntés függhet egyéb tényezőktől is, mint hogy kitől jött az objektum és milyen információt tartalmaz.

A megőrzési stratégiák kifejlesztése és használatának módszertana az elektronikus levéltár tevékenységének a kulcseleme. Ennek során a levéltár kidolgozza azoknak a beavatkozásoknak a kereteit, amelyeken keresztül az iratok megőrzését hosszú távon biztosítani tudja. A megőrzési stratégiák során a kidolgozás, fenntartás mellett a digitális objektumokra típusonként azonos megoldásokat lehet alkalmazni.

2.2.2.1. Migráció

A migráció az elektronikus iratok hosszú távú megőrzésének legelterjedtebb stratégiája, az elavult régi dokumentumformátumok konverzióját jelenti újabb, használatban lévő formátumokra. Előnye, hogy az esetek többségében képes megnyújtani a digitális forrás olvashatóságát, legalább addig, amíg az újabb formátum is elavulttá válik. A migrációhoz – akár tömeges beavatkozásokhoz is - könnyen elérhető, egyszerűen használható eszközök állnak rendelkezésre. A mig-

ráció hátránya, hogy torzíthatja, vagy megváltoztathatja a digitális objektum eredeti megjelenését, struktúráját, jelentését és viselkedését. Miután a beavatkozás külön-külön érint minden egyes objektumot, a tömeges migráció esetén a hibák és torzulások felderítetlenek maradnak. Az évek során egymást követő migrációs beavatkozások egymás negatív hatásait felerősíthetik, és jelentős adatvesztést okozhatnak. A migrációt sokan hasonlítják a fénymásoláshoz: jobb vagy rosszabb eszközökkel jobb vagy rosszabb másolatot készíthetünk az eredetiről, az információvesztés azonban minden esetben szükségszerűen bekövetkezik. A digitális állományvédelem növekvő mértékben kezdi felismerni az eredeti bitsorozat megőrzésének fontosságát, ezért a kutatások növekvő szerepet juttatnak más stratégiának, illetve a migrációs stratégia komplexebb, kifinomultabb alkalmazásának. A stratégia egyik változatában a levéltár az eredeti bitsorozat megtartása mellett, a felhasználás pillanatában végzi el a migrációt, a levéltárhasználók körében aktuálisan használt formátumokra (héjmodell). Az eredeti bitsorozat megőrzése így biztosítja az integritást és a hitelességet és szükségtelenné teszi a migrációs ciklusokat. A módszer hátránya hogy az eljáráshoz a migrációs eszközök széles körét kell létrehozni, fenntartani és alkalmazni.

2.2.2.2. Emuláció

A stratégia lényege, hogy a levéltár nemcsak az adatot, de a létrehozásához/használatához szükséges programokat is megőrzi, a technológiai avulást pedig az eredeti hardver/szoftverkörnyezet szoftveres szimulációjával hidalja át. A megvalósíthatósággal kapcsolatos aggályok mellett az emuláció hátránya, hogy az eredeti alkalmazás megőrzése valójában szükségtelen az archiválási feladatokhoz, hiszen a teljes funkcionalitás fenntartása nem szükséges az adatok értelmezéséhez, hiszen világos, hogy annak érdekében, hogy megőrizzük magát a fényképet nem szükséges megőriznünk a képszerkesztő alkalmazást valamennyi szerkesztési, módosítási, transzformálási funkciójával.

A másik hátrány, hogy az eredeti program kizárólag az eredeti módon jeleníti meg az adatokat, ami behatárolja azok használatát, nem is beszélve arról, amikor az eredeti alkalmazás nem rendelkezik megfelelő exportálási funkcióval.

Az emulációnak ugyanakkor kétségtelen előnye, hogy az eredeti bitsorozat változatlanságával a hitelességnek a konverziós megoldásoknál magasabb szintjét képes megvalósítani, hiszen az integritást direkt módon, az autenticitást pedig közvetve biztosítja. Ez lényeges előny azoknál az iratoknál ahol a hitelesség megőrzése különösen fontos. Szintén az emulátorok mellett szól a tradicionális levéltári megközelítés, amely az iratokat minél teljesebb eredeti megjelenési formájukban, kontextusukban igyekszik megőrizni. (Rothenberg 1999. 17-26)

Az emulációs környezetek alapvetően két réteg emulációját oldhatják meg külön-külön, vagy integráltan:

Az operációs rendszer emulátorok olyan szoftverek, amelyek aktuális operációs rendszer környezetbe ágyazva előállítják egy-egy korabeli operációs rendszer (MSDOS Windows változatok (3.1, 95, NT, XP) minél pontosabb szoftveres leképezését, így fölöttük működőképessé válnak az adott szoftver környezetre tervezett és abban üzemszerűen működtetett alkalmazói szoftverek. Létező megoldások: Windows emulátor (WINE), DOS emulátor (DOSEMU), FreeDOS.

A hardver emulátorok olyan szoftverek, amelyek aktuális operációs rendszer környezetbe ágyazva előállítják egy-egy korabeli hardver platform (x86 16, 32 bit) és specifikáció minél pontosabb szoftveres leképezését és így fölöttük működésre képesek lesznek az adott hardver specifikáció mellett tervezett és üzemszerűen működtetett operációs rendszerek. Az egyes emulátorok három jellemző paramétere a támogatott befogadó operációs rendszer, az emulált hardver platform és a támogatott beágyazott operációs rendszer. Ezek használata olyan esetekben indokolt például, amikor az emulált hardver paraméterek, méretek, időzítések jelentős hatással lehetnek a futtatni kívánt alkalmazói szoftverre, vagy a alkalmazói szoftver olyan operációs rendszer környezethez kötődik, aminek már nincs sem a aktuális hardvereken karbantartott változata, sem pedig aktuális operációs rendszerek fölött futóképes szoftveres emulációja. Létező megoldások: Xen, Dioscuri nyílt forrású emulátor, Bochs nyílt forrású emulátor, HyperV, VMWare kereskedelmi virtualizációs megoldások.

2.2.2.3. Egyéb megoldások

Megőrző koncepció

A digitális világ beköszöntekor a levéltárak egyik legkorábbi félelme az volt, hogy a gyorsan avuló eszközök megőrzésére képtelenek lesznek. A migrációból adódó ellentmondások, az információs technológia paradigmaváltásai nyilvánvalóan nem okoznak problémát, ha mindazok a gépek, eszközök, operációs rendszerek és alkalmazások, amelyek az elektronikus irat eredeti környezetét jelentették, maradéktalanul rendelkezésre állnak. Valószínűtlen persze, hogy a régi gépek a végtelenségig üzemeltethetők lesznek, hogy ennek költsége megfizethető lehet, de még ha mindez megvalósulna is, ez a megoldás a használatot a világ néhány kiválasztott helyére korlátozná. (Székely 2005. 133-134.o.) Bár a mikroprocesszorok integrált áramköreinek meglehetősen korlátozott az élettartamuk, ha az eszközök nagy része fenntartható is, az adathordozó elkerülhetetlenül tönkremegy. Az pedig igen valószínűtlen, hogy egy hetvenes években használt 8-inches floppyn tárolt szövegfájl biztonsági másolatát a 21. század elején hasonló médiára másolják, nem pedig DVD-lemezre, amelyet viszont a fájl eredeti hardverkörnyezete magától értetődően nem tud kezelni.

A technikatörténeti múzeumot megőrző stratégia nem alkalmas arra, hogy az eredeti adat változatlan formában megőrzését biztosítsa, a hosszú távú megőrzésben azonban mégis fontos szerep jut neki. Egyfelől a gondatlanul kezelt adathordozók adatainak megmentése csak az elavult eszközpark fenntartásával lehetséges. A levéltáraknak természetesen nem kell maguknak gondoskodniuk az elméletileg elgondolható teljes digitális archeológiai környezetről – bár a legáltalánosabb esetekre nyilvánvalóan fel kell készíteni őket. (Rothenberg 1999. 9-10. o)

Fizikai másolat készítése.

A hosszú távú megőrzés egyik problémája az elektronikus média korlátozott élettartama. A mesterséges öregítési tesztek a gyártók optimizmusa ellenére az optikai lemezek élettartamát néhány évre becsülik, míg a hagyományos hordozók, mint a pergamen és a papír századok óta szolgálnak adattárolásra. A fizikai másolat készítésének hátránya, hogy bizonyos iratokról egyáltalán nem készíthető, mivel azok nem a kinyomtatás szándékával készültek. A fizikai másolat nem képes reprodukálni az elektronikus állomány valamennyi lényeges tulajdonságát, az irat elveszti interaktív, dinamikus jellegét, jelentősen csökken a kereshetőség, kommunikálhatóság, reprodukálhatóság.

A kezdetben a könyvtári katalógusok biztonsági másolatára alkalmazott COM eljárás (Computer out on microfilm) arra épít, hogy a mikrofilmek különösen jó eredményeket érnek el a tartóssági vizsgálatok során, élettartamuk akár az 500 évet is meghaladhatja a megfelelő tárolási feltételek biztosítása mellett. Előnyük, hogy nagyításon keresztül az emberi szem számára közvetlenül olvashatók, a digitális iratok teljes funkcionalitását pedig automatizált visszadigitalizáláson keresztül biztosítják, amely történhet akár a kép, akár a mikrofilmen tárolt bitsorozat beolvasásával. A megoldás nemcsak a formátumkonverziókat teszi feleslegessé, de lehetővé teszi az adatobjektum és a metaadatok együttes tárolását – így fizikailag hozva létre az OAIS-nak megfelelő információs csomagot – és nagy biztonságot nyújt a hitelesség fenntartására is, mivel a mikrofilmek nehezen manipulálhatók.(Nestor Handbuch Kap. 8.32-8.33)

A megőrzési stratégiák alkalmazása nem zárja ki egymást egyetlen levéltáron belül sem és mind az együttes alkalmazásuk, mind az egyes levéltári anyagokra való egyedi alkalmazásuk a leginkább járható út az iratok hosszú távú megőrzése érdekében. Az ezzel kapcsolatos szabályozásnak ugyanakkor világosnak, átfogónak, naprakésznek és hozzáférhetőnek kell lennie.

2.2.2.4. A levéltár rendelkezzen archiválási szabályzatában dokumentált megőrzési stratégiákkal és legyen képes megőrzési terveinek felülvizsgálatára. (MOT_MEGORZSTRAT)

A levéltár vagy levéltári rendszernek korszerű, alapos és dokumentált megőrzési stratégiákkal kell rendelkeznie. Ezek tipikusan az információ értelmezésének (a formátumokat is ide értve) elavulását célozzák és a véletlen vagy szándékos adatvesztés megelőzését szolgálják. Amennyiben a migráció a kiválasztott megközelítés ezeken a területeken, szükséges arra vonatkozó stratégia, hogy mi váltja ki a migrációt és milyen típusú migráció szükséges minden egyes azonosított megőrzési feladat megoldásához. A levéltárnak reagálnia kell a technológiafigyelésből és a rendszer monitorozásából eredő információra, amiből egyes esetekben a levéltár által tárolt anyagok kezelési módjának nem várt megváltoztatásával is következhet. A levéltárnak képesnek kell lennie bemutatni, hogy képes felülvizsgálni a hosszú távú terveit a változó körülmények függvényében. [TRAC B3.1, B3.3, PLEDGE PP-0001]

2.2.2.5. A levéltárnak meg kell határoznia a befogadható illetve az archiválásra alkalmas fájlformátumok körét (MOT_FORMATUM)

Az iratok hosszú távú megőrzése során az egyik legnagyobb kihívás a fájlformátumok elavulásának kezelése. A közlevéltárak esetében ezt célszerű központilag szabályozni, a magánlevéltárak maguk határozzák meg a befogadható illetve archiválásra alkalmas fájlok körét. Valamennyi levéltárnak törekednie kell a fenntartható fájlformátumok befogadására és a sokféleség csökkentésére. A szabályozást megelőzően keletkezett iratok tekintetében meg kell különböztetnie azoknak a fájloknak a körét, amelyeket képes SIP-ként befogadni és feldolgozni azoktól a formátumoktól, amelyek a hosszú távú megőrzésre alkalmasak.

A hosszú távú megőrzésre alkalmas fájlok tulajdonságait több kutatás vizsgálta. Legújabban a Digital Preservation Coalition jelentése igyekezett szintetizálni a korábbi kutatások eredményét. Ezek alapján a hosszú távon megőrizhető fájlok kiválasztásakor a következő szempontokat kell mérlegelni:

- elfogadottság, vagyis hogy a fájlformátum mennyire elterjedt.
- technológiafüggőség, vagyis hogy a formátum mennyire támaszkodik más technológiákra
- nyilvánosság, vagyis hogy a formátumspecifikáció nyilvános-e,
- átláthatóság, vagyis, hogy mennyire könnyen azonosítható és ellenőrizhető a tartalma
- metaadatok, vagyis, hogy vannak-e metaadatok a formátumon belül.

(Todd 2009. 2.o.)

A szöveges dokumok tekintetében a korai szabványok a TXT és az RTF formátumot, az ausztrál VERS szabvány a TXT és a PDF/A használatát támogatja, a holland nemzeti levéltár Digital

Longevity osztálya a PDF és XML formátumok használatát tekinti a leghatékonyabb módnak, hogy hosszú távon biztosítsa a szöveges állományok megőrzését. Az XML előnyei és hátrányai ebben az esetben kiegészítik a PDF-ét. Egyfelől viszonylag könnyű megőrizni a szöveges dokumentum megjelenését PDF-ben, miközben ezt bonyolult megoldani XML-ben. Másfelől az XML a PDF-nél könnyebben alakítható a kontextuális információ és az explicit struktúra megőrzésére és az XML-en alapuló fájlformátumok (ODF, OOXML) lehetőséget adnak arra, hogy az irat keletkezése hosszú távon megőrizhető formában történjen. A PDF konverzióra jelenleg az Adobe Acrobat a legmegbízhatóbb konverziós eszköz, de számos vizsgálható független eszköz is rendelkezésre áll.

Mind a holland Digital Preservation Testbed3, mind a belga eDAVID4 mind pedig az angol InSpect[5] projekt eredménye az volt, hogy e-mailek rövid és hosszútávú megőrzésének leginkább megfelelő stratégiája az XML-be való konverzió. Erre számos eszköz alkalmas, XMaiL, XENA, ReadPST

Hosszú távon a legmegfelelőbb megközelítés az adatbázisok megőrzésére az XML-be való konverzió, bár sokan a relációs adatbázist önmagában is szabványos megoldásnak tekintik, ami az XML-nél nagyobb lehetőséget kínál nagy méretű adatbázisok megőrzésére. 2009-ben jelent meg a svájci Bundesarchiv adatbázisok megőrzésére alkalmas XML formátuma a .siard

Audió állományok archiválására a Microsoft és az IBM által fejlesztett .wav (waveform audio file) konténerformátum terjedt el, amely tömörített és tömörítetlen audió adat tárolására is alkalmas, utóbbit használják gyakrabban. A Linear Pulse Code Modulation (LPCM) elterjedt, tömörítetlen veszteségmentes algoritmus a formátumban, amely széles körben elfogadottá teszi a .wav formátumot az archiválással foglalkozó szervezetek körében.Az mp3 (MPEG-1 Audio Layer3) szintén széles körben elterjedt formátum, amely az emberi hallásra optimalizált, nem veszteségmentes tömörítési eljárást alkalmaz. A JHOVE alkalmas eszköz mind a karakterizációra, mind a konverzióra. Az utóbbi időben terjed a FLAC (free lossless audio codec), amely nyílt forrású, veszteségmentes tömörítési eljárást alkalmaz.

---

3 From digital volatility to digital permanence – preserving e-mail. The Hague. 2003

4 http://www.edavid.be/

5 Egyesült Királyság Nemzeti Levéltárának InSpect (Investigating Significant Properties of Electronic Content) projektje http://www.significantproperties.org.uk/

A raszterképek megőrzésére a levéltárak hagyományosan tömörítetlen TIFF fájlokat használnak, mindazonáltal érdemes megjegyezni, hogy az InSpect projekt a GIF fájlok esetében találta a legtartósabbnak a metaadatok megőrzését. Mivel a képek a legáltalánosabb digitális objektumok közé tartoznak számtalan eszköz van a megjelenítésükre és konverziójukra. A konverziót magas szinten támogatja az Adobe Photoshop, a nyílt forrású GIMP, és a JHOVE.

2.2.2.6. A levéltárnak meg kell határoznia a levéltári megőrzés során az iratok leírására használt metaadatok szabványait. (MOT_METAADAT)

Az OAIS szabvány az információs csomagok szerkezetének meghatározásával definiálta azokat az adatterületeket, amelyeket az adatobjektummal együtt kell rögzíteni. A levéltárnak meg kell határoznia, hogy az egyes területeken milyen metaadatokat használ és rögzítenie kell a használattal kapcsolatos konvenciókat.

Konténer szabványok:

- METS - A Kongresszusi Könyvtár által fenntartott információs csomag szabvány, ami magában foglalja a leíró, adminisztratív, viselkedési, megőrzési metaadatokat, lehetővé teszi, hogy ezeknek az elemeknek a leírására a csomag készítője más szabványokat (Dublin Core, EAD, PREMIS stb.) használjon fel. http://www.loc.gov/standards/mets/
- XFDU – XML Formatted Data Unit. A Consultative Committee for Space Data Systems által készített információs csomag szabvány.
  http://sindbad.gsfc.nasa.gov/xfdu/pdfdocs/xfduspec.pdf

Általános tartalmi leíró szabványok

- Dublin Core - Egymélységű, tartalomleíró metaadatszabvány, tizenöt – minősítők használatával kiterjeszthető - alapattribútummal. Egyszintű leírásra alkalmas, ezért levéltárakban elsősorban darabjegyzékek készítése során használják. Az alapinformációk egységes használata és egyszerűsége miatt elterjedt, de levéltári használata során korlátot jelent az egyszintű leírás, és a minősítők sokfélesége, ami részben a hierarchikus leírást és a szabványos adatcserét korlátozza. MSZ 15836 számon. http://dublincore.org/
- EAD – Encoded Archival Description, a Kaliforniai Egyetem által fejlesztett és a Kongresszusi Könyvtár által fenntartott XML alapú leíró és adatcsere szabvány a levéltári segédletek leírására. Levéltári területen általános adatcsere szabvánnyá vált, miután a levéltári anyag leírására is alkalmas és kompatibilis az ISAD(G) leíró szabvánnyal.
  http://www.loc.gov/ead/eaddev.html

Speciális tartalmi leíró szabványok

- EAC-CPF – Az EAC-CPF (Encoded Archival Context-Corporate Bodies, Persons, Families) XML szabvány a levéltári anyaggal kapcsolatos testületek, személyek és családok leírására. A szabványt a Society of American Archivists és a Berlini Állami Könyvtár tartja fenn. http://eac.staatsbibliothek-berlin.de/
- MIX - A Kongresszusi Könyvtár által fenntartott komplex, hierarchikus leíró és adatcsere szabvány a digitális képgyűjtemények technikai információinak leírására, amely az adatok és szerkezet tekintetében a Data Dictionary - Technical Metadata for Digital Still Images (ANSI/NISO Z39.87-2006) szabványra épít. http://www.loc.gov/standards/mix/

Technikai adatokat leíró szabványok

- PREMIS – A Kongresszusi Könyvtár által fenntartott leíró séma és adatcsere szabvány a megőrzési metaadatok (PDI) leírására. http://www.loc.gov/standards/premis
- LMER - (Long-term preservation Metadata for Electronic Resources) A Német Nemzeti Könyvtár által az Új-Zélandi Nemzeti Könyvtár szabványán alapuló technikai metaadatok adatcseréjére kifejlesztett XML alapú leíró séma http://www.d-nb.de/eng/standards/lmer/lmer.htm

2.2.2.7. Az elektronikus levéltárnak meg kell határoznia azokat a tulajdonságokat, amelyeket a digitális objektumokból megőriz. (MOT_MEGORZOTTTUL)

A digitális objektumok öt jellemző tulajdonsága a tartalom, a kontextus, a megjelenés, a szerkezet és a viselkedés. A megőrzendő tulajdonságok kiválasztása függ a levéltár megőrzési lehetőségeitől, a megőrizni kívánt iratok jellemzőitől és a megőrzés céljától. Jellemző döntési helyzet egy dokumentum teljes képi megfelelőségének vagy teljes szövegű keresésének dilemmája. Az elektronikus levéltár dönthet párhuzamosan mindkét formában való megőrzésről. A belső szabályozás kialakításánál tekintettel kell lenni a vonatkozó jogszabályokra és az azokban rögzített átadási szabályokra. [TRAC B1.1, Nestor 9.2, PLEDGE PP-0001]

2.2.2.8. Szükségesek megfelelően alkalmazott monitoring és értesítési mechanizmusok annak jelzésére, amikor az értelmezési információ (RI) az elévülés közelébe ér vagy már nem fenntartható. (MOT_RIELEVULES)

Az elektronikus iratok megőrzésében az egyik legáltalánosabb problémát az információ megőrzéséhez szükséges értelmezési információ (RI) kezelése jelenti. Ez tartalmazhatja az információt a fájlformátumok kezeléséről és az értelmezésükhöz vagy feldolgozásukhoz alkalmazható szoftverekről. Az eredeti formátumot konvertálni kell, ha a levéltár az elavult formátumot nem tudja tovább kezelni. Az értelmezési információ megváltoztatása jelentheti az adott formátum feldolgozásához szükséges szoftverre vonatkozó információ megváltoztatását az eredeti formátum megtartása mellett. A levéltárnak rendelkeznie kell a közelgő elavulásokra figyelmeztető

aktív mechanizmusokkal. Az elévülés összefügg a levéltárhasználók tudásbázisával (milyen eszközökkel rendelkeznek, milyeneket tudnak használni). [TRAC B3.2, PLEDGE PP-0014]

2.2.3. TÁROLÁS, ŐRZÉS (TAR)

Az AIP-ok hosszú távú megőrzésének megvalósítására minimális feltételrendszer vonatkozik. A rendszer infrastruktúrája (a tárolási infrastruktúra műszaki követelményeit a 2.3 fejezetben tárgyaljuk) megfelelő szolgáltatásokat kell, hogy nyújtson az AIP-on végzett magasabb szintű levéltár funkcióknak (objektumkezelés), hogy az megbízhatóan hajtsa végre feladatait. De amennyiben a magasabb szintű funkciók nem használják ezeket a szolgáltatásokat, vagy nem megfelelően használják azokat, a megőrzés nem biztosítható.

2.2.3.1. Aktív módon ellenőrizni kell az egyes AIP-ok integritását. (TAR_AIPINTEGR)

Az OAIS terminológiáját használva ez azt jelenti, hogy a levéltárnak rendelkeznie kell változatlansági információval (Fixity Information, FI) az AIP-pal kapcsolatban amely alapján az AIP-ok integritását ellenőrzi. A változatlansági információt (FI), (vagyis az ellenőrző összegeket és az AIP-okkal való kapcsolatukat), az AIP-tól elkülönülten kell tárolni és védeni, annak érdekében, hogy, aki rosszhiszeműen megváltoztat egy AIP-ot, ne legyen képes a változatlansági információt is megváltoztatni. A levéltárnak naplóznia kell az ellenőrzések végrehajtását. [PLEDGE PP-0016]

2.2.3.2. Rendszeresen szükséges ellenőrizni az archívum egészének integritását. (TAR_ARCHINTEGR)

Az AIP integritását magasabb szinten is ellenőrizni kell biztosítva, hogy valamennyi AIP, amelynek léteznie kell valóban létezik, és hogy nincs olyan tárolt AIP, amely nem szerepel a nyilvántartásban. Az ellenőrzőösszeg önmagában nem képes ennek igazolására. [TRAC B4.5, PLEDGE PP-0016]

2.2.3.3. A tárolásnak biztosítania kell a fizikai megőrzést és az AIP-ok olvashatóságát. (TAR_AIPOLV)

A levéltárnak megfelelő módszereket és eszközöket kell használnia az archív objektumok megfelelő tárolása és olvashatósága érdekében. Az olvashatóság itt azt jelenti, hogy a tárolóeszközről a megfelelő bitsorozat kiolvasható. [Nestor 10.3]

2.2.4. ADATKEZELÉS (ADATK)

Minden levéltár kritikus összetevője az információkezelési funkcionalitás. Tekintet nélkül a levéltár anyagára, méretére vagy jellegére a levéltári nyilvántartó rendszernek képesnek kell lennie tárolni, nyomon követni és használni az elektronikus levéltár alapfunkcionalitását támogató metaadatokat. Az OAIS modell ezt a funkcionalitást az Adatkezelésen (Data Management) keresztül írja le, ám a gyakorlatban ez az információ más funkciók számára is fontos, hiszen az

adatok nem önállóan, hanem a befogadás, tárolás, megőrzéstervezés és használat során jönnek létre. Ebből kifolyólag a követelményjegyzék ebben a fejezetben csak a leíró adatokkal szorosan összefüggő, máshol nem említett követelményeket fogalmazza meg.

A levéltárhasználók a levéltártól azt várják, hogy minél könnyebben megtalálják az információt a levéltári anyagban. A levéltár minimális metaadat követelményeinek ezért illeszkednie kell levéltárhasználói közösség minimális elvárásaihoz. Ez nem azt jelenti, hogy a levéltárnak képesnek kell lennie minden egyes felhasználó igényeinek megfelelő katalógus információt nyújtani, fel kell viszont mérni, hogy egy átlagos levéltárhasználó milyen információt szeretne megkapni és azok létrehozásáról a hasznosság és a költségek függvényében kell dönteni.

Amennyiben a levéltár több különböző, jól meghatározó csoportot is kiszolgál, (pl. családfakutatók), akkor a metaadat követelmények lehetnek eltérőek a levéltári anyag különböző területein. A metaadat tartalmazhat bármilyen információt, amelyet a potenciális használó hasznosnak találhat, beleértve azoknak az eszközöknek a jelzését is, amelyek a használathoz szükségesek.

A levéltár feladata biztosítani, hogy minden egyes eltárolt objektumhoz tartozik leíró információ.

2.2.4.1. Az elektronikus levéltár a nyilvántartásain keresztül biztosítsa, hogy a levéltári nyilvántartás egésze és a vegyes iratok kezelése a fond egységének elve alapján történik. (ADATK_VEGYESIR)

A levéltári nyilvántartásnak lehetővé kell tennie, hogy a felhasználó vegyes iratokon alapuló leírási egységeket is létrehozzon.

Valamennyi leírási egység (fond, állag, sorozat) leírása (metaadatai) a meghatározó jelentéseken, lekérdezéseken keresztül legyen egységesen elérhető, függetlenül attól, hogy a levéltári anyag (adatobjektum) elektronikus, vagy hagyományos. A nyilvántartásnak lehetővé kell tennie a vegyes iratok egymásra vonatkozásának rögzítését, az erre vonatkozó adatok fenntartását és megjelenítését. A levéltári nyilvántartásnak biztosítania kell, hogy a papíralapú, az elektronikus, illetve a vegyes ügyiratok bármely kombinációban egymáshoz rendelhetők legyenek

A nyilvántartás biztosítsa, hogy az elektronikus iratokra jellemző metaadatok rögzíthetők, karbantarthatók és visszanyerhetők legyenek.

2.2.4.2. A levéltárnak közzé kell tennie a levéltári anyag minimális metaadat-követelményeit, amelyek lehetővé teszik a felhasználók számára az érdeklődésükre számot tartó anyagok elérését. (ADATK_MAKOZZETETEL)

A visszakereséshez és leíráshoz szükséges metaadatok előírását tartalmazhatja jogszabály (a tanúsított iratkezelő szoftverek esetében a 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet, vagy a gyarapodáshoz és törzskönyvezéshez szükséges metaadatok tekintetében a 10/2002. (IV. 13.) NKÖM rendelet, de előírhatja azt szabvány (ISAD(G)) vagy a levéltár archiválási sza-

bályzata. Az egyes információs objektumok típusainak megfelelő metaadat-sémák képesek biztosítani a különböző információs objektumok (video, email, GIS) leírását, ezeket a levéltárnak el kell készítenie.

A levéltárnak a metaadatok tekintetében sem kell megfelelnie valamennyi elképzelhető igénynek, de teljesítenie kell az olyan típusú igényeket, amelyek a levéltárhasználók részéről hangsúlyozottan jelentkeznek. [TRAC B5.1, PLEDGE PP-0004]

2.2.4.3. A levéltár a feldolgozás során rögzíti a levéltári metaadatokat és biztosítja, hogy azok az archív objektumhoz (AIP) társításra kerülnek. (ADATK_MAROGZITES)

A levéltár előírhatja az iratképző számára, hogy az iratokkal együtt szolgáltassa a metaadatokat (pl. a KIB 28. ajánlásnak megfelelően), visszautasítva az átvételt, amennyiben azok hiányosak, vagy saját maga rögzítheti – egészítheti ki – a metaadatokat a befogadás során. A levéltárnak szabályoznia kell a metaadatok létrehozásával kapcsolatos munkafolyamatokat, egyértelművé téve, hogy ezzel kapcsolatban kinek mi a feladata. A metaadatoknak az objektumokhoz való társítása fontos, de nem igényel egy-az-egyhez megfeleltetést és nem szükséges valamennyi metaadatot az AIP-pal együtt tárolni. A hierarchikus leírási sémák lehetővé teszik, hogy néhány leíró elem több egységgel legyen társítható. A metaadat-AIP kapcsolatnak elválaszthatatlannak kell lennie, további kapcsolatok létrehozása során sem veszhet el. [TRAC B5.2, PLEDGE PP-0004]

2.2.4.4. A levéltárnak létre kell hoznia és meg kell őriznie hivatkozási integritást valamennyi archív objektum (AIP) és a hozzá tartozó metaadatok között. (ADATK_MAHIVINT)

Az AIP és a metaadatok közötti dokumentált kapcsolatnak kell lennie, a rendszerdokumentáción, a műszaki architektúrán, az eljárások munkafolyamatainak dokumentációján alapulva meg kell valósítani a hivatkozási integritás megteremtését és megőrzését valamennyi archív objektum (AIP) és a hozzá tartozó metaadatok között.

Valamennyi AIP-nak rendelkeznie kell leíró információkkal és valamennyi leíró információnak legalább egy AIP-ra kell mutatnia, hogy az integritás megfelelő legyen. Kiemelt figyelmet kell szentelni azoknak a műveleteknek, amelyek az AIP-okra és azonosítóikra vannak hatással és arra, hogy ezek során a műveletek során hogyan biztosítható az integritás fenntartása. Különösen az AIP javítását, módosítását követően, biztosítani kell a régi leíró metaadatok megőrzését, az állandó azonosítók perzisztenciáját. [TRAC B5.3, B5.4, PLEDGE PP-0006, PLEDGE PP-0019]

2.2.5. LEVÉLTÁRI FELDOLGOZÁS (FELD)

Az AIP-ok megőrzésének a 2.2.2 fejezetben tárgyalt és az ottani követelményeknek megfelelő dokumentált megőrzési stratégiákat kell a gyakorlatban megvalósítania, ezek tipikusan konver-

ziók, transzformációk, checksum ellenőrzések, levéltári rendezés, leírás, selejtezés, a feldolgozás történetének követése amelyek mind hatással vannak a megőrzés megbízhatóságára.

2.2.5.1. A levéltár megőrzi az archív objektumok (AIP-ok) tartalmi információit (CI) (FELD_TARTMEGORZ)

A levéltárnak képesnek kell lennie arra, hogy bemutassa, hogy az AIP-ok hűen tükrözik azt a tartalmat, ami a befogadás során beérkezett, és hogy bármilyen ezt követő, vagy a jövőben tervezett transzformáció meg fogja őrizni a levéltár állományának ezt a szempontját. Szükséges megőrizni a kapcsolatot az eredeti befogadási folyamat eredményeként létrejött és a további transzformációk eredményeként létrejött vagy megváltozott valamennyi új AIP változat között. A végrehajtástól függően ezek az újabb objektumok lehetnek teljes egészében újak vagy csupán frissített AIP-ok. Az állandó kapcsolatot a befogadott objektum és az AIP között minden esetben fenn kell tartani. A levéltárnak bármely konkrét digitális objektum vagy objektumok csoportja esetén képesnek kell lennie az AIP láncolat bemutatására. A levéltárnak a feldolgozás során meg kell őriznie az AIP-ok és a nem AIP-okban tárolt metaadataik kapcsolatát, az AIP-on belüli hivatkozások integritását tekintet nélkül arra, hogy tisztán elektronikus vagy vegyes iratokról van szó. [TRAC B4.3, PLEDGE PP-00017]

2.2.5.2. A levéltár a migráció során ellenőrzött és tesztelt, szilárd gyakorlaton alapuló beavatkozásokat hajt végre (FELD_MIGR)

Egy levéltár valószínűség szerint több megőrzési stratégiát fog alkalmazni. A különböző stratégiák alkalmazhatók a digitális objektumok különböző típusai szerint és/vagy több stratégia alkalmazható egyetlen objektumtípusra. Ennek összefüggéseit azonban mind az archiválási stratégiában, mind az AIP metaadatai között rögzíteni kell.

A tartalmi információ (CI) migrációja során, beleértve a fájlformátumokat, adatszerkezetet, a levéltárnak olyan állományvédelmi beavatkozásokat kell végrehajtania, amelyek kellőképpen dokumentáltak, ellenőrzöttek és megfelelőségüket széles körű teszteredmények támasztják alá. Ennek érdekében felhasználhatók más levéltárak módszertani eredményei. Pl. Ilyen például a Planets projekt6 http://testbed.planets-project.eu/testbed/ [TRAC B4.1, B4.2, B4.3 PLEDGE PP-0015]

---

6 A Planets (Preservation and Long-term Access through Networked Services) projekt az Európai Unió 6. keretprogramja által támogatott négyéves (2006-2010) projekt az elektronikus információ hosszútávú megőrzésére alkalmas gyakorlati szolgáltatások és eszközök fejlesztésére. is a four-year project co-funded by the European Union under the Sixth Framework Programme to address core digital preservation challenges. A könyvtárak, kutatóintézetek és magáncégek

2.2.5.3. A levéltár rögzíti kell az AIP megőrzését érintő beavatkozások és adminisztrációs folyamatok metaadatait. (FELD_BEAVROGZ)

Ezeket az adatokat az AIP létrehozással kapcsolatos tevékenységekkel egyidejűleg, és összefüggésben azokkal a beavatkozásokkal, amelyre vonatkoznak kell létrehozni. Az adatok létrejöhetnek automatikus módon vagy rögzíthetők emberi beavatkozás segítségével, az általuk leírt tevékenység természetétől függően. [TRAC B4.5, PLEDGE PP-0007]

2.2.5.4. A vegyes iratok együttes kezelését a feldolgozás során is érvényesíteni kell. (FELD_VEGY)

Azokat az irategyütteseket, amelyekben papír alapú iratok és elektronikus iratok összetartozó módon vannak jelen, csak együttes rendezési terv alapján szabad rendezni. Az AIP-okon végzett beavatkozások során figyelemmel kell lenni arra, hogy az esetleges változásokat (rendezés, selejtezés) a papír alapú iratokon is érvényesíteni kell. Lehetséges stratégia a rendezés során a papíralapú iratok digitalizálása és ezt követően a digitalizált és digitálisan keletkezett iratok együttes kezelése.

2.2.5.5. A levéltárnak selejteznie kell nem maradandó értékű elektronikus állományait. (FELD_SEL)

A levéltárnak selejtezési eljárás alá kell vonnia azokat a SIP-eket, amelyek értelmezése nem biztosítható, azokat az AIP-okat, amelyek redundánsak és megőrzésük szükségtelenné válik. A selejtezés a levéltári anyag selejtezésének általános szabályai szerint történik.

A levéltári nyilvántartásnak figyelmeztetnie kell a felhasználót arra, ha a selejtezés alá vont elektronikus iratra egy másik – papír alapú vagy elektronikus - irat hivatkozik (van a két irat között e rendszerben létrehozott kapcsolat) és le kell állítania a selejtezési eljárást az alábbi korrekciós intézkedések valamelyikének megtételéig:

a) a megfelelő jogosultságú felhasználó a folyamat folytatását vagy megszakítását kezdeményezi,

b) jelentés készítése az érintett ügyiratok vagy iratok részleteiről és az összes hivatkozásról, amelynek a selejtezési eljárás alá vont irat a célobjektuma.

A levéltár ennek során rögzíti a selejtezéssel kapcsolatos beavatkozások és adminisztratív folyamatok metaadatait.

---

részvételével folyó programban részt vesz Hollandia, az Egyesült Királyság és Svájc nemzeti levéltára. A projekt legfontosabb eredménye a PLATO megőrzéstervezést támogató eszköz és az elektronikus állományvédelmi beavatkozások közösségi alapú tesztelését támogató PLANETS TESTBED (http://www.planets-project.eu/.)

[10/2002. (IV. 13.) NKÖM rendelet 3.§.]

2.2.5.6. A selejtezett levéltári anyag megsemmisítésének helyreállíthatatlannak kell lennie (FELD_TÖRL)

2.2.6. A JÓVÁHAGYOTT SELEJTEZÉSI JEGYZŐKÖNYVET KÖVETŐEN AZ ELEKTRONIKUS LEVÉLTÁRI ANYAG VALAMENNYI ÁLLOMÁNYÁT ÚGY KELL MEGSEMMISÍTENI, HOGY AZ EREDETI TARTALOM SEM TELJESEN, SEM RÉSZLEGESEN NE LEGYEN HELYREÁLLÍTHATÓ.HOZZÁFÉRÉS, HASZNÁLAT (HASZN)

A levéltárak méretük, technikai felszereltségük, kutatóforgalmuk, levéltári anyaguk nagy változatossága miatt a levéltárhasználati feltételek a lokális alkalmazhatóság és értelmezés körébe tartoznak. Valamennyi elektronikus levéltárnak képesnek kell lennie az állományából olyan információs csomagot létrehozni (Dissemination Information Package, DIP) és a jogosult levéltárhasználó rendelkezésére bocsátani, amely egyértelmű kapcsolattal rendelkezik az archívumban őrzött levéltári anyaggal.

2.2.6.1. A levéltár kutatótermi szabályzatában rögzíti az elektronikus iratok használatának feltételeit. (HASZN_KUTSZAB)

A levéltár szabályzatainak rögzíteniük kell az archívum által őrzött információ használatának feltételeit és különböző módjait. Lehetővé kell tenni, hogy a felhasználók megismerhessék a szabályzatokat és azok következményeit. A felhasználóknak tudniuk kell, hogy mit, mikor és hogyan kérhetnek és ezeknek milyen költségei lehetnek. A levéltár kutatói rendszerének teljes egészében meg kell felelnie a kutatási szabályzatnak és ezt a hozzáférési igények naplóállományain és nyomkövetésén keresztül igazolnia is kell tudni [TRAC B6.1, 6.5, PLEDGE CU-0007]

2.2.6.2. *A megőrzési szolgáltatások kialakításához meg kell határozni a levéltárhasználói igényeket (HASZN_FELHCSOP)*

A levéltárnak meg kell határoznia azokat a felhasználói csoportokat, amelyek levéltári anyagát használják (pl. iratok keletkeztetői, érintettek, tudományos kutatók, családfakutatók, helytörténészek). A felhasználói csoportok eltérő elvárásai és lehetőségei hatással vannak a levéltár munkájára a megőrzés és a szolgáltatás végrehajtásakor. A levéltárhasználók elvárása nem csupán a hozzáférés biztosítása, hanem az információ értelmezhetőségének biztosítása, ami hatással lesz a digitális objektum kezelésére és a teljes levéltár technikai infrastruktúrájára. Egy adott iratátvétel során a levéltárnak definiálnia kell a használat értelmezhetőségének paramétereit, ami csak a levéltárhasználói közösség ismeretében lehetséges.

Az értelmezhetőség dokumentációja tipikusan tartalmazza a levéltárhasználók által az információval kapcsolatban használni kívánt szoftverek meghatározását, a kutatóteremben biztosítandó eszközöket.

Amennyiben a levéltárhasználók vagy annak igényei, tudásbázisa az idők során változnak, a levéltárnak szolgáltatásait a változásokhoz kell igazítania. [TRAC 3.1, Nestor 1.3, PLEDGE OEL-0014]

2.2.6.3. *A levéltárnak biztosítania kell a felhasználók számára a digitális objektumokban lévő információ megfelelő használatát. (HASZN_DIGOBJINF)*

Az elektronikus levéltár elsődleges célja, hogy biztosítsa a digitális objektumokban lévő információ az aktuális és jövőbeni használatát a levéltárhasználók számára. A digitális objektumok használata megőrzésükön, hozzáférésükön és értelmezhetőségükön alapul. [Nestor 2., PLEDGE CU-0003]

2.2.6.4. *A levéltár biztosítja kell, hogy a levéltárhasználói közösség hozzáfér a digitális objektumokhoz. (HASZN_HOZZAFBIZT)*

A levéltárnak biztosítania kell, hogy a jogosult felhasználók hozzáférhessenek a digitális objektumokhoz. Biztosítania kell a megfelelő kutatási lehetőségeket is. A szolgáltatások meghatározásánál számításba kell venni a felhasználói csoportok igényeit. A levéltárnak előzetesen értesítenie kell a felhasználókat a használat feltételeiről és költségeiről. A díjszabásokat áttekinthető módon hozzáférhetővé kell tenni.

A hozzáférés magában foglalja.

- A digitális objektumokhoz való hozzáférést,
- Analóg másolat készítését és szolgáltatását (egy dokumentum nyomtatott változatát),
- Digitális másolat készítését és szolgáltatását (letöltést a felhasználó tárhelyére, vagy kutatóteremben adathordozóra való kiírását)

[Nestor 2.1]

2.2.6.5. *A levéltárnak biztosítania kell, hogy a levéltár használói értelmezni tudják a digitális objektumokat (HASZN_ERTELM)*

A levéltárnak biztosítania kell, hogy a digitális objektumok hosszú távon értelmezhetők legyenek, így meg kell teremtenie a használat szükséges alapfeltételeit. Ebbe beleértendő mind az adatobjektumok, mind a metaadatok interpretálhatósága. A megvalósítás során a levéltárnak figyelembe kell vennie a levéltárhasználók igényeit. Minél inkább speciális tartalomról van szó, annál valószínűbb, hogy speciális technikai eszközökre lehet szükség (mint például tervezői, térinformatikai szoftverek).

A levéltárhasználók és az egyes levéltárhasználói csoportok változásai hatással vannak az objektumok értelmezhetőségére. A levéltárnak rendszeresen ellenőriznie kell, hogy az objektumok a levéltárhasználók számára értelmezhetők. [Nestor 2.2, PLEDGE CU-0003]]

2.2.6.6. A levéltárnak rögzítenie kell valamennyi használati esemény (beleértve a kérőlapokat, megrendeléseket stb.) adatait (HASZN_NAPLOZAS))

A levéltárnak a jogszabályokban előírt és a kérések teljesítéséhez szükséges adatokat kell rögzítenie. A korlátozással nem érintett anyagok publikus hozzáférése során ez akár azt is jelentheti, hogy csekély vagy éppen semmilyen információ nem kerül rögzítésre a hozzáférésről. A levéltárnak a fejlesztés szempontjából ebben az esetben is szüksége lehet statisztikai információra arról, hogy milyen anyagok kerültek használatra, de arról nem, hogy azt kik használták. [TRAC B6.2, PLEDGE CU-0009]

2.2.6.7. Biztosítani kell, hogy a felhasználók csak olyan iratokat kaphatnak meg, amelyre vonatkozóan rendelkeznek hozzáférési jogosultsággal. (HASZN_JOGOSULTSAG)

A levéltárnak képesnek kell lennie az iratokhoz tartozó hozzáférési korlátozások és használati feltételek egyértelmű kezelésére és annak nyilvántartására, hogy az egyes AIP-okra milyen korlátozások vonatkoznak. A levéltárnak képesnek kell lennie a levéltárhasználók azonosítására annak érdekében, hogy megállapítsa a jogosultság fennállását.

A használati feltételek alatt általában azt értjük, hogy ki láthatja az iratokat, természetesen ezek a feltételek azonban tartalmazhatják, hogy az iratokról milyen feltételek mellett készíthető másolat, vagy milyen feltételek mellett használható fel különböző célokra. Különösen a szerzői joggal érintett iratok vagy a letéti megállapodás keretében a levéltárban őrzött iratok használati feltételei tartalmazhatnak ilyen korlátozásokat.

A levéltár on-line szolgáltatásán keresztül azonosítás nélkül is hozzáférést biztosíthat a minden korlátozás nélkül megismerhető iratokhoz.

Amennyiben a hozzáférési feltételekből az következik, hogy a felhasználóknak a DIP-ek kézhezvételét megelőzően nyilatkozniuk kell a használatról, a levéltárnak biztosítania kell a nyilatkozatok rögzítését. Ez történhet a kutatóteremben aláírt űrlapokon, vagy annak igazolásával, hogy egy nyilatkozat online formában elolvasásra került és egy gomb lenyomásával a beleegyezés megtörtént. Ez lehet adatkezelési nyilatkozat vagy lemondás a tartalom üzleti célú felhasználásáról. [TRAC 6.3, PLEDGE CU-0008]

2.2.6.8. A levéltárnak képesnek kell lennie a felhasználók azonosítására, amikor ezt a levéltári anyag használata megköveteli. (HASZN_FELHAZON)

Az azonosítás módja a felhasználás során vagy az AIP-ok tekintetében is lehet különböző. A jogszabályok a levéltári anyag hozzáféréséhez gyakran erős autentikációt írnak elő. Az azonosítás történhet a kutatóteremben való személyes megjelenés során személyazonosító okmány bemutatásával vagy távoli eléréssel Ügyfélkapun keresztül a 225/2009. (X.14.) Korm. sz. rendelet 28 § szerint. Amennyiben jogszabály nem ír elő erős azonosítást egyes iratok hozzáférhetővé

tétele során, a levéltár kialakíthatja a felhasználói azonosítás egyszerűbb módjain keresztül is, mint pl. egy felhasználónév és egy kapcsolódó jelszó, vagy a kezdeményezés forrás IP címe, illetve más mechanizmus a szükséges biztonság fokától függően. A levéltárnak biztosítania kell, hogy a hozzáférési és az iratok kiadására vonatkozó szabályok a gyakorlatban érvényesüljenek, és hogy az azonosítással kapcsolatos engedélyezések szintje összhangban legyen azzal a kockázattal, ami a téves vagy hiányos azonosításból fakad. Némely korlátozás jogszabályokból származik, másokat esetleg a letéti megállapodások írnak elő.

A levéltárosoknak szintén szükséges alkalmilag hozzáférnie a tárolt objektumokhoz, az iratátvétel, a megőrzési beavatkozások végrehajtása, az ellenőrzések, konverziók vagy a DIP-ek készítése során. A levéltárnak legyenek az információbiztonsági és adatvédelmi szabályzatában rögzített mechanizmusai a tárolt objektumoknak a személyzet által elkövetett szándékos vagy véletlen rongálásai elleni védelmére. [TRAC B6.4, PLEDGE CU-0008]

2.2.6.9. A kikért digitális objektumokat a kérésnek megfelelően kell összeállítani. (HASZN_DIGIOBJOSSZ)

Amennyiben a jogosult levéltárhasználó az iratoknak egy adott halmazát kéri, a levéltárhasználónak meg kell kapnia a teljes halmazt. Amennyiben a jogosult levéltárhasználó egy fájlt kér, meg kell kapnia a teljes fájlt. Ha az igénye nem teljesíthető, erről értesíteni kell, és az elutasítást a levéltárhasználó számára meg kell indokolni. Nem elfogadható, ha a kérés csak részben került teljesítésre, a hiányos DIP kézbesítésre került, de nem egyértelmű a kutató számára, hogy a teljesítés csak részleges.

A DIP összeállítása során, amennyiben transzformáció szükséges, a megfelelő beavatkozásokat kell végrehajtani. Sokszor összetettebb transzformációkra lehet szükség az AIP-okból a DIP-ek létrehozására, ezért a DIP készítését a kérőlapok és a DIP készítés naplófájljai alapján a levéltárnak igazolnia kell tudni. [TRAC B6.7, B6.8]

2.2.6.10. Valamennyi kutatási kérést teljesíteni kell vagy formálisan el kell utasítani. (HASZN_OSSZESKERES)

Egy kutatási kérés lehet sikeres vagy sikertelen és azt is korlátozni kell, hogy mennyi idő telhet el, amíg a kutató erről értesítést kap. A kérőlap-nyilvántartáson, a DIP készítés naplófájljain és a hozzáférési naplóállományokon keresztül ellenőrizhetővé kell tenni, hogy valamennyi kutatási kérés teljesült vagy hivatalosan elutasításra került [TRAC B6.9, PLEDGE CU-0009]

2.2.6.11. A felhasználó kérésére az anyagról hiteles másolatot kell készíteni az eredeti alapján vagy az eredetire visszavezethető módon. (HASZN_MASOLAT)

A levéltár használójának bizonyosnak kell lennie azzal kapcsolatban, hogy az eredeti objektum megbízható másolatát kapta vagy legalábbis az visszavezethető valamilyen ellenőrizhető módon

az eredeti objektumra. Ez a megkülönböztetés azért szükséges, mivel az objektumok nem mindig azon a módon, ugyanabban a csoportosításban kerülnek kiadásra, mint ahogy azt a levéltár átvette. Egy adatbázis részeként meglévő sorok oszlopok és táblák úgy kerülnek kiadásra, hogy a hiteles másolatnak csekély jelentése van. A befogadás és a megőrzési beavatkozások megváltoztathatják a fájlformátumokat vagy egyesíthetnek, illetve szétválaszthatják az eredetileg átadott objektumokat.

A megkülönböztetés a hiteles másolatok és a visszavezethető objektumok között szintén fontos, amikor transzformációk kerülnek alkalmazásra. A levéltár felelőssége a hitelesség biztosítása tekintetében csak az iratok átvételével kezdődik, ezért a hitelességi láncnak csak a befogadásig kell visszamennie, de néhány iratnál ennél tovább is visszavezethető hitelességi láncot is szükséges lehet biztosítani.

A levéltárnak archiválási szabályzatában általános szinten rögzítenie kell azokat az elveket, amelyek mentén a DIP-et a megfelelő AIP-ból létrehozza. Az AIP-DIP létrehozási folyamat meghatározó része, hogy a DIP-ek mi módon tükrözik megbízható és konzisztens módon az AIP-ok tartalmát és így az eredeti anyagot.. A DIP-ek lehetnek az AIP-ok egyszerű másolatai, vagy készülhetnek egy AIP egyszerű formátumkonverzióján keresztül. Más esetekben ezek komplex módon származhatnak több AIP-ból is.

[TRAC 6.10]

2.3. Műszaki és biztonsági követelmények

A levéltár műszaki követelményei nem írnak elő konkrét hardvereket vagy szoftvereket, az AIP-ok hosszú távú megőrzéséhez, de leírják az infrastruktúra és biztonság főbb, általános követelményeit. Az itt felsorolt kritériumok erősen támaszkodnak az információbiztonsági szakterület mértékadó dokumentumaira, ezek közül is meghatározóan az ISO 17799 és ISO 27001 szabványokra, kiemelve a levéltár számára fontos követelményeket, de szükségtelenül nem ismételve az ott leírtakat.

A követelmények a következő csoportokba sorolhatók:

- Infrastruktúra követelményei. Általános rendszerinfrastruktúra követelmények és az archiválásra megfelelő technológiák biztosítása, amelyek a rendszerinfrastruktúra követelményekre épülve, további követelményeken keresztül meghatározzák átvételhez, archiváláshoz és a levéltár felhasználói számára nyújtott szolgáltatások számára megfelelő technológiák és stratégiák kialakításával és fenntartásával kapcsolatos követelményeket. (INF)

- Biztonsági követelmények. Magukban foglalják a biztonsági tervezés, szabályozás követelményeit a fizikai biztonságtól az IT rendszereken keresztül - mint amilyenek a szerverek, tűzfalak, routerek - a tűzvédelmi rendszereken, vízbetörés-érzékelőkön keresztül egészen azokig a rendszerekig, amelyek emberi közreműködéssel működnek. Továbbá megfogalmazzák a katasztrófakezelés és helyreállítás általános követelményeit és a biztonsági incidensek kezelésének általános elveit.
- Kockázatelemzés (KOCK)
- Információ-biztonság (INFBIZT)
- Fizikai és környezeti biztonság (FIZB)
- Azonosítás és hitelesítés (AZON)
- Hozzáférés-ellenőrzés (HOZZ)
- Adatvédelem (ADATV)
- Katasztrófatűrés (KAT)
- Mentés, helyreállítás, elvárt redundanciák (MENT)
- Incidenskezelés (INC)

2.3.1. INFRASTRUKTÚRA KÖVETELMÉNYEI (INF)

Biztonságos és megbízható infrastruktúra nélkül a digitális objektumokon végrehajtott beavatkozások nem lehetnek megbízhatók. A magyarországi közlevéltárak méretüket, feladatkörüket, levéltári anyagukat és személyi állományukat tekintve jelentősen különböznek. Jelen követelmények megfogalmazásakor figyelemmel kellett lenni arra, hogy a követelmények valamennyi közlevéltárra érvényesíthetők legyenek. A követelmények szándékoltan általánosak, hogy egyaránt teljesíthetők legyenek a Magyar Országos Levéltár és egy egyfős egyetemi levéltár rendszerének implementációja során is.

2.3.1.1. A levéltár rendelkezzen a szolgáltatásaihoz szükséges, biztonságos hardver- és szoftvertechnológiával. (INF_HWSW)

A levéltárnak ismernie kell, hogy a felhasználók milyen szolgáltatásokat várnak el tőle, figyelnie és értékelnie kell a rendszer használatát annak érdekében, hogy a szolgáltatási igények változásait felmérje és a rendszer hardver és szoftverkörnyezetét ezekhez a változásokhoz igazítsa. Az elektronikus levéltári rendszer hardver és szoftverkomponenseinek biztosítania kell:

- hogy megfelelően képesek legyenek támogatni iratátvételi, ellenőrzési, tárolási, nyilvántartási, megőrzési, és használati szolgáltatásait (megfelelőség)
- hogy a rendszerben található adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további

felhasználásának megakadályozása az adatkezelést szabályozó törvényi előírások betartásával történjen (törvényes adatkezelés);
- a rendszerben kezelt adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhessék meg, használhassák fel, illetve rendelkezhessenek a felhasználásáról (bizalmasság);
- a rendszerben kezelt adat tartalma és tulajdonságai az elvárttal megegyezzenek - ideértve a bizonyosságot abban, hogy az elvárt forrásból származik és a származás megtörténtének bizonyosságát is -, továbbá a rendszerelemek a rendeltetésüknek megfelelően használhatóak legyenek (sértetlenség);
- a rendszerben kezelt adatokat, illetve az informatikai rendszer elemeit az arra jogosultak a szükséges időpontban és időtartamra használhassák (rendelkezésre állás);
- érvényesüljön az összes releváns fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, megszakítás nélkül megvalósuló zárt, teljes körű és folytonos védelem, amely akockázatokkal arányos.

[TRAC C2.1, 2.2, PLEDGE TI-0003, PLEDGE TI-004]

2.3.1.2. A rendszernek biztosítania kell a levéltár belső rendszereivel és a releváns külső rendszerekkel való interoperabilitást. (INF_IOP)

A rendszer együttműködési képessége egyfelől általános követelményként fogalmazódik meg a levéltár felépítésével, a digitális objektumok kezelésével és a levéltárban alkalmazott műszaki megoldásokkal szemben. Az interoperabilitás technológiai aspektusa vonatkozik egyrészt a homogén rendszerek összekapcsolhatóságára, másrészt -- éppen az (SZK_SZABV) követelmény szerinti szabványosságon keresztül -- a más rendszerekkel való minél mélyebb szintű integrálhatóságra is vonatkozik. A rendszernek illeszkednie kell a releváns elektronikus közszolgáltatásokhoz (Ügyfélkapu, Hivatali Kapu, e-fizetés) és a KIB 28. ajánlásához.

2.3.1.3. Megfelelő kapacitású hardverek és szoftverek szükségesek a levéltár szolgáltatásának biztosítására, a tárolt adatok őrzésére, a digitális objektumoknak a hozzáférés-ellenőrzéssel való összekapcsolására, a biztonsági mentés támogatására. (INF_KAPACITAS)

A levéltárnak a jelenlegi szolgáltatásaihoz elegendő és a növekedési tervében meghatározott kapacitásig skálázható infrastruktúrával kell rendelkeznie az egyes rendszerfunkciók tekintetében. A levéltár legyen képes demonstrálni a folyamatoknak, a hardver és szoftvereszközöknek, a biztonsági másolatokat kezelő rendszereknek a megfelelőségét. [TRAC C1.2, PLEDGE TI-002]

2.3.1.4. *A levéltárnak nyilván kell tartania valamennyi digitális objektum másolatainak példányait és azok elhelyezését. (INF_PELDANYOK)*

A levéltárnak képesnek kell lennie valamennyi tárolt digitális objektum összes példányának az azonosítására és minden egyes objektum és azok másolatai helyének meghatározására. Ez alatt az azonos – biztonsági célú - másolatok és nem az objektumok AIP készítés során létrejött különböző változatai értendők. Az elhelyezést úgy kell leírni, hogy az objektum helye pontosan, félreérthetetlenül meghatározható legyen. Ez lehet egy abszolút fizikai elhelyezés vagy egy logikai elhelyezés a tárolóeszközön a tárolás alrendszerén belül. A levéltárnak lehetnek különböző eljárásai a különböző objektumosztályok tekintetében, olyan jellemzőkön alapulva, mint az iratképző, az információ típusa, vagy annak értéke. [TRAC C1.3, PLEDGE TI-0011]

2.3.1.5. *Biztosítani kell a digitális objektumok minden példányának szinkronizálását. (INF_SZINKRON)*

Amennyiben több másolat létezik, biztosítani kell, hogy az objektumok szándékos változtatásai átvezetésre kerülnek az objektum valamennyi másolatán. Szükséges információt biztosítani arról, hogy mikor fejeződik be a szinkronizálás és ideális esetben rendelkezni kell egy előzetes becsléssel arról, hogy mennyi időt vesz igénybe. Attól függően, hogy ez automatikus, vagy emberi beavatkozást igényel (mint például egy távoli tárolón lévő másolat kikérése) a szükséges idő másodpercektől akár több hétig is terjedhet. Szükséges rögzíteni, hogy mi történik a szinkronizálás alatt. Ennek a katasztrófa esetén történő visszaállítás során van szerepe. Amennyiben egy objektum másolata megváltozik és a szinkronizálás egybeesik egy katasztrófaeseménnyel, lényeges megbizonyosodni arról, hogy a frissítés sikeresen átvezetésre került. [TRAC C1.4, PLEDGE TI-0011]

2.3.1.6. *A levéltárnak rendelkeznie kell hatékony mechanizmussal az adatvesztés és adatsérülés észlelésére. (INF_ADATVESZTES)*

A levéltárnak pontosan észlelnie kell az esetlegesen bekövetkező adatvesztést, biztosítva, hogy minden veszteség a szabályzatokban rögzített tűréshatáron belül marad. Az adatvesztést észlelni kell a hiba okára való tekintet nélkül. Ez alkalmazandó az adatsérülések valamennyi formájára és körére, beleértve a hiányzó objektumokat vagy a sérült, helytelen vagy valótlan objektumokat, az objektumon belüli sérüléseket és a hibák másolását az adatkonverzió vagy a másolatok szinkronizációja során. Ideális esetben a levéltár képes demonstrálni az archívum integritását, vagyis hogy valamennyi AIP megvan, aminek meg kell lennie, nincs többlet, és hogy mind a digitális objektumok mind pedig ezek valamennyi metaadata sérülésmentes.

A megközelítésnek dokumentáltnak és ellenőrzöttnek kell lennie, mechanizmusokkal olyan tipikus kockázatok mérséklésére, mint a hardverhibák, emberi tévedések vagy rosszindulatú beavatkozások. Ha a levéltár erre általánosan elismert mechanizmusokat használ, mint például az

MD5 függvények, nyílt forrású ellenőrző megoldások (pl. md5sum, tripwire), csak a konkrét használatukat kell dokumentálnia. Amilyen mértékben használ saját fejlesztésű, egyedi megoldásokat, olyan mértékben kell a hatékonyságukat is meggyőzően alátámasztania, hogy az adatvesztés és sérülés a szabályzatban megállapított tűréshatáron belül észlelhető. Az adatvesztéseket elég gyorsan kell felismerni ahhoz, hogy a rendszeres hibaforrások, mint a hardverhibák ne vezessenek a hibák felhalmozódásához és ne okozzanak a tűréshatáron túli adatvesztést.

Valamennyi – időlegesen – elvesztett adatot helyre kell tudni állítani a biztonsági mentésekből. [TRAC C1.5, PLEDGE PP-0016]

2.3.1.7. A levéltárnak jelentést kell készítenie valamennyi adatvesztésről/sérülésről és a sérült vagy elveszett adatok helyreállítása/visszaállítása érdekében megtett lépésekről. (INF_ADATVESZTDOK)

A levéltárnak dokumentálnia és a lehetőségek szerint javítania kell az adatok integritását sértő valamennyi eseményt. A rendszernek képesnek kell lennie arra, hogy értesítse a rendszeradminisztrátorokat valamennyi naplózott problémáról. Ezeket az eseményeket, visszaállítási műveleteket és azok eredményeit jelenteni kell az adminisztrátoroknak, az adatoknak megjeleníthetőeknek kell lenniük. A levéltár dokumentálja azokat az eljárásokat is, amelyek az adatvesztés vagy sérülés észlelése esetén követ, beleértve a visszaállítás eredményességének mérésére alkalmazott eljárásokat. Valamennyi, az eljárások részeként az objektumok helyreállítására irányuló műveletet naplózni kell. Az állománynak elérhetőnek kell lennie. [TRAC C1.6]

2.3.1.8. A levéltár rendelkezzen előzetesen dokumentált eljárásrenddel a tárolóeszközök és a hardverek cseréjére. (INF_HARDVERCSERE)

A levéltárnak pontos információval kell rendelkeznie arról, hogy a tárolóeszközök migrációjára vonatkozó beavatkozások - a tárolóeszközök cseréje és az adatok migrációja - mennyi időt vesznek igénybe (a bitsorozat átalakítása nélküli másolás az egyes médiák között). Fontos, hogy az érintett folyamatok annak ellenőrzését is magában foglalják, hogy a másolás megfelelően történt-e.

A levéltáraknak figyelemmel kell kísérniük a rendszerben lévő valamennyi hardverkomponens vagy azok bármelyikének elavulását, ami szükségessé teheti a migrációt. Elavult rendszerek üzemeltetésénél nehéz biztosítani a rendszer egyre növekvő karbantartási igényét, ez a levéltár számára kockázatot jelent, a gyártó vagy szolgáltató támogatásán túli működtetés növeli a levéltári anyaggal kapcsolatos kockázatot. [TRAC C1.7, PLEDGE TI-0014]

2.3.1.9. A változáskezelési eljárások során azonosítani kell azokat a kritikus területeket és rendszereket, amelyek változásai hatással lehetnek a levéltár kötelező feladatainak teljesítésére. (INF_KRITRSZ)

Az iratátvételt, adatkezelést, használatot, tárolást, és biztonságot érintő változásokat csak változáskezelési eljárással szabad megvalósítani. A megbízható archiválás során szükséges annak dokumentálása, hogy a rendszerben milyen változások, mikor történtek meg. A nyomon követhetőség lehetővé teszi annak megértését, hogy a rendszernek egy konkrét változása mire volt hatással.

A változáskezelési folyamatok részeként szükséges megoldást biztosítani a kritikus rendszerek változásaiból következő hatások tesztelésére. A kritikus rendszerek változásait, amikor lehetséges elkülönülten előzetes tesztelésnek kell alávetni, a várható viselkedés dokumentálásával és a visszavonási eljárások elkészítésével. A változásokat követően el kell végezni a rendszer vizsgálatát a váratlan és elfogadhatatlan viselkedés ellenőrzésére. Amennyiben ilyen viselkedés kimutatható a változást és valamennyi következményét vissza kell vonni. A teljes rendszertesztelés vagy az egyes egységek tesztelése vonatkozhat erre a követelményre, az összetett biztonsági tesztek nem szükségesek. A tesztelés ugyan drága, de szükséges felismerni, hogy a teljesen nyílt rendszer, ahol a változások soha nem kerülnek értékelésre vagy tesztelésre biztosan problémákat okoznak.

A szoftverfrissítések alkalmazásával kapcsolatos döntések nagy valószínűséggel kockázatelemzési folyamat eredményeként születnek. A szoftverkiegészítések gyakran felelősek a rendszer funkcionalitásának vagy teljesítményének hiányosságaiért. Nem szükséges, hogy egy levéltár valamennyi szoftverkiegészítést implementáljon, mindegyiknek az alkalmazását meg kell fontolni. Minden implementált frissítést, részletesen dokumentálni kell a végrehajtás módjára vonatkozóan is, akár automatikus, akár manuális frissítésről van szó. A biztonsági frissítések összefügghetnek az operációs rendszertől különböző szoftverekkel, mint az adatbázis-alkalmazásokkal, webszerverekkel, ezeket szintén dokumentálni kell. [TRAC C1.8, 1.9, 1.10, PLEDGE TI-0013]

2.3.2. KOCKÁZATELEMZÉS (KOCK)

2.3.2.1. Rendszeres kockázatelemzést kell végezni a rendszer kritikus elemeire, mint az adatok, rendszerek, személyek, fizikai és biztonsági igényeknek. (KOCK_EL)

A levéltárnak rendszeres időszakonként (legritkábban évente, vagy a szervezetben bekövetkező jelentős változások esetén) általános kockázatelemzést kell végeznie, hogy azonosítsa, számszerűsítse és szervezeti célok és kockázatelfogadási kritériumok alapján sorolja be a releváns kockázatokat. A kockázatelemzés során az elektronikus levéltári sajátosságaiból adódóan in-

formatikai kockázatelemzést is kell végezni. A kockázatelemzés során széles körben elfogadott kockázatelemzési módszert (pl. ITB 8. sz. ajánlás, COBIT) kell alkalmazni.

Az ITB 8. sz. ajánlásának eljárásrendje a következő négy szakaszra építi fel a kockázatelemzést

1. Védelmi igény feltárása,

2. Fenyegetettség elemzés,

3. Kockázatelemzés,

4. Kockázatmenedzselés

A védendő területek számbavételét követően a fenyegetettség elemzés során fel kell mérni az egyes alapfenyegetettségeket. Általánosságban az elektronikus levéltárban az informatikai rendszerek életciklusából adódó kockázatok, adatvesztés, illetéktelen hozzáférés és manipuláció, a tapasztalatlanságból eredő személyi kockázatok jelentik a legnagyobb veszélyt ugyanakkor nem jelentős mértékű kockázat a szolgáltatáskiesés. Emellett a következő jellemző fenyegetettségekkel szükséges számolni.

- környezeti infrastruktúra területén: ellenőrizetlen belépés, betörés, közműellátás zavarai, tűz, vízbetörés,
- eszközök hardverek területén: érzékenysége az elektromágneses sugárzással szemben, hibás kezelés, áramellátás zavarai, műszaki jellegű hibák, rendellenességek,
- adathordozók területén: nem védett tárolás, szakaszos demagnetizálódás hosszabb tárolás esetén, tárolóképesség,
- dokumentumok területén: hiányzó dokumentumok
- szoftverek területén: felhasználói azonosítás hiánya, hozzáférési jogok helytelen odaítélése, szükségtelenül biztosított jogok, hiányzó naplózás, helytelen jelszó-mechanizmus, ártalmas kódok
- az adatok területén: hiányzó hibakezelési eljárás, hiányzó ellenőrző eljárás, sértetlenség, bizalmasság elvesztése, hitelesség elvesztése, működőképesség elvesztése
- a kommunikáció területén: lehetőség az üzenetek lehallgatására, meghamisítására
- a személyek területén: felmondás, hibás viselkedés az ismeretek hiánya miatt, hiányos biztonságtudat miatt, szándékos hibás viselkedés.

A kockázatelemzés során fel kell mérni és értékelni a kárkövetkezményeket, amelyek a levéltárban jellemzően adatvesztés, személyes adat megsértése, bizalomvesztés, időhöz kötött adatok idő előtti nyilvánosságra hozatala, károk a törvények megsértése miatt, adatvédelmi törvény megsértése, szerzői jogi törvény megsértése, a közmegbecsülés elvesztése, illetve dologi károk.

A károk értékelése, három meghatározó szempont alapján történhet. Ezek a következôk:

- a károk egyedi nagyságrendje (értékskála),
- a károk valószínû bekövetkezési gyakorisága (gyakoriság skála),
- a kárérték és a gyakoriság által keletkezô kockázat (kockázatmátrix).

A kockázatelemzést biztonsági intézkedéseknek kell követniük, amelyek biztosítják, hogy a rendszer védelme arányban legyen a kockázatokkal.

A DRAMBORA (Digital Repository Audit Method Based on Risk Assessment) kifejezetten elektronikus levéltárak kockázatelemzésére és kockázatkezelésére alapozott audit módszertan. Kérdéskészlet helyett belső használatra készült munkafolyamaton keresztül biztosítja, hogy a levéltár maga ismerje fel és azonosítsa a folyamatainak jellemzőit és kockázatait, rögzítse és fejlessze ki ezek kezelését. Maga az audit egy 10 lépésből álló folyamat. A kockázat elemzés során alkalmazható kockázat valószínűségek és kockázat hatások besorolásának definíciói rögzítettek és mérőszámokkal leírhatóak – egytől hatig illetve egytől hétig terjedő skálán. Az audit első hat lépése a szervezet által dokumentálandó tételekre vonatkozik, míg az utolsó két lépés a 7. és a 8. lépés során feltárt kockázatok feldolgozásának és kezelésének a témaköre. [TRAC C3.1, NHHE 5.1, PLEDGE TI-0012]

2.3.3. INFORMÁCIÓBIZTONSÁG (INF.BIZT. POLITIKA, AZ INF.BIZT. SZERVEZETE] (INFBIZT)

2.3.3.1. A levéltárnak rendelkeznie kell információbiztonsági szabályzattal (INFBIZT_IBSZ)

A levéltárnak rendelkeznie kell érvényes, a gyakorlatban alkalmazott, a működés követelményeinek, valamint a vonatkozó jogszabályoknak megfelelő információbiztonsági szabályzattal, a levéltárnak biztosítania kell ennek ismeretét és érvényesítenie kell a betartását. Az információbiztonsági szabályzatot meghatározott időközönként (legritkábban évente), illetve lényeges változások bekövetkezésekor át kell vizsgálni annak biztosítására, hogy továbbra is alkalmas, helytálló és hatékony maradjon.

[MSZ ISO/IEC 27001:2006 A5.1.1, A5.1.2, NHHE 5.2, PLEDGE TI-006]

2.3.3.2. Rendszeres biztonsági ellenőrzést kell végezni. (INFBIZT_ELL)

A levéltárnak a vonatkozó szabályzatban (pl. IBSZ) meghatározott rendszerességgel biztonsági ellenőrzést kell végeznie. Az ellenőrzés során feltárt hiányosságoknak visszacsatolással kell rendelkezniük a kockázatelemzés és a szabályozási folyamatokra.

A szolgáltatással kapcsolatos szervezeti és műszaki változások, illetve biztonsági esemény esetén saját hatáskörben soron kívüli felülvizsgálatot valósít meg.

Az ellenőrzés, valamint a megtett intézkedések felülvizsgálata során tapasztalt hiányosságok esetében az illetékes vezető a kiemelt kockázatot jelentő - azaz adatvesztés, vagy adatokhoz való jogosulatlan hozzáférés veszélyét felvető - hiányosság esetén a szolgáltatást azonnal felfüggeszti, Nem kiemelt kockázatot jelentő hiányosság esetén határidőt határoz meg a hiányosság megszüntetésére. Egy rendszerelem üzemeltetésének vagy felfüggesztett szolgáltatásának újraindítása - a hiányosságok megszüntetését követően is - csak az illetékes vezető engedélyével történhet.
[TRAC C3.2]

2.3.4. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG (FIZB)

2.3.4.1. Biztosítani kell az elektronikus levéltár helyiségeinek és információinak fizikai védelmét (FIZB_HOZZ)

A biztonsági vonatkozású szabályzatok által és azok alkalmazása során biztosítani kell a levéltár helyiségeinek és információinak védelmét, a jogosulatlan, illetéktelen fizikai behatolás, károkozás és zavarkeltés megakadályozása érdekében. Azokon a területeken, ahol információkat vagy információ-feldolgozó eszközöket tartanak, biztonsági határzónákat (lehatároló védfalakat, kártyával ellenőrzött beléptető kapukat, illetve személyzettel ellátott portaszolgálatot) kell alkalmazni e területek védelmére. A biztonsági területeket a belépés megfelelő ellenőrzésével kell védeni, hogy e területekre csak a belépésre jogosultak juthassanak be. Az irodák, helyiségek és létesítmények fizikai védelmét ki kell alakítani és azt alkalmazni kell. Az off-line iratátvétel munkaterületeit, és egyéb olyan pontokat, amelyeken keresztül arra jogosulatlan egyének a helyiségekbe bejuthatnak, ellenőrizni kell, és lehetőség szerint, ezeket az illetéktelen hozzáférés megelőzése érdekében el kell különíteni az információ-feldolgozás létesítményeitől. Ki kell alakítani és alkalmazni kell a biztonsági területeken történő munkavégzésre vonatkozó fizikai védelmet és irányelveket. Ki kell alakítani a tűzvész, áradás, földrengés, robbanás, polgári zavargás, valamint a természeti és ember által előidézett katasztrófák más formái által okozott károk elleni védelmet és azt alkalmazni kell. [MSZ ISO/IEC 27001:2006 9.1.]

2.3.4.2. Biztosítani kell az elektronikus levéltár berendezéseinek védelmét (FIZB_BER)

A vagyontárgyak elvesztésének, károsodásának, eltulajdonításának, illetve megrongálásának, valamint a szervezeti működés fennakadásának megelőzése érdekében az elektronikus levéltár berendezéseit úgy kell elhelyezni, illetve védeni, hogy csökkenjen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége. A berendezéseket védeni kell a közüzemi létesítményekben bekövetkező meghibásodások okozta áramkimaradásoktól és más zavaroktól. Az adatátvitelt bonyolító, illetve az információszolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell a lehallgatástól és a

károsodástól. A berendezéseket előírásszerűen karban kell tartani folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében. Valamennyi olyan berendezést, amely tároló-eszközt foglal magában, ellenőrizni kell annak biztosítása érdekében, hogy az érzékeny adatok és engedélyezett szoftverek a selejtezést megelőzően eltávolításra, illetve biztonságos felülírásra kerüljenek. Berendezések, információk, illetve szoftverek előzetes engedély nélkül nem vihetők ki a telephelyről. [MSZ ISO/IEC 27001:2006 9.2]

2.3.5. AZONOSÍTÁS ÉS HITELESÍTÉS (AZON)

2.3.5.1. Az elektronikus levéltár rendszereinek meg kell követelniük minden felhasználótól az azonosítást (AZON_KIKENYSZERIT)

Sikeres azonosításnak kell megelőznie az adott felhasználó vagy a felhasználó munkaköre nevében történő bármely művelet végrehajtásának az engedélyezését. A felhasználó kijelentkezése után kötelező az újbóli azonosítás. Hitelesítő adatok használatakor, ezeknek egyedieknek kell lenniük, és nem lehet többször kiadni őket. Hitelesítési adatra példa a (felhasználói név, jelszó) páros. Jelszóalapú azonosítás esetén meg kell határozni a jelszavakkal kapcsolatos konkrét követelményeket (pl. jelszóhossz, karakterkészlet, lejárati szabályok). A visszaélés lehetőségének további korlátozása lehetséges automatikus kijelentkeztetés használatával, megadott inaktivitást követően, a tranzakció lezárásával vagy egy lehetséges időn túl. [NHHB IA 1, PLEDGE TI-0009]

2.3.5.2. A rendszernek képesnek kell lennie az azonosítási hibák kezelésére (AZON_SIKERTELEN)

A megbízható rendszereknek meg kell akadályozniuk a további azonosítási kísérleteket, ha a sikertelen kísérletek száma elér vagy meghalad egy maximumként meghatározott értéket (javasolt érték: 3-5). Ha a sikertelen azonosítási kísérletek száma eléri vagy meghaladja a megengedett kísérletek maximális számát, és rendszer-adminisztrátori munkakörről van szó, akkor megfelelő más csatornán értesítést (pl. SMS riasztás, figyelmeztető üzenet) kell generálni. [NHHB IA 2]

2.3.6. HOZZÁFÉRÉS-ELLENŐRZÉS (HOZZ)

2.3.6.1. A rendszernek meg kell akadályoznia a rendszerfunkciókhoz és a tárolt objektumokhoz való illetéktelen hozzáférést. (HOZZ_RENDSZFUNKC)

A rendszerhozzáférés ellenőrzési funkciói azt felügyelik, hogy csak meghatalmazott személyek használhassák a megbízható rendszerek objektumait (tárolt adatokat, rendszerfunkciókat stb.). Ez az elektronikus levéltár valamennyi rendszerfunkciójára és objektumára alkalmazandó, amely valamilyen hozzáférési korlátozást tartalmaz.

2.3.6.2. Az elektronikus levéltár munkatársainak körülhatárolt szerepeiknek, feladat- és hatásköreiknek kell lenniük a rendszerben végrehajtott műveletekkel kapcsolatban. (HOZZ_SZEREPKOR)

Szükséges annak meghatározása, hogy az elektronikus levéltár munkatársai közül, ki mit csinálhat a rendszerben. Ki adhat hozzá felhasználókat, kinek van hozzáférése a metaadatok megváltoztatására, ki tekintheti meg a naplóállományokat. Fontos a hatáskörök értékelése, és annak vizsgálata, hogy a munkatársak megértik, mire van felhatalmazásuk. A rendszernek képesnek kell lennie az elektronikus levéltár munkatársainak jogosultságkezelésére. Egyetlen adatkeresési vagy adat-visszanyerési művelet sem tárhat fel a felhasználó számára olyan információkat (metaadatot vagy irattartalmat), melyre a felhasználónak nincs jogosultsága. [TRAC C3.3, PLEDGE TI-0008]

2.3.7. ADATVÉDELEM (ADATV)

2.3.7.1. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie a levéltárnak. (ADATV_SZEMADAT)

Az Adatvédelmi törvény szerint az adatkezelők felelőssége az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével okozott kárért objektív, ezért a személyes adatok védelme a levéltárban fokozott körültekintést igényel. A követelményt egyaránt alkalmazni kell a levéltári anyagban lévő személyes adatokra és a levéltári anyag használatával, kapcsolatban keletkezett személyes adatokra is. [Avtv. 10. § (2), EKINT 4., PLEDGE CU-0002]

2.3.7.2. A rendszert úgy kell kialakítani, hogy személyes adatok csak akkor legyenek összekapcsolhatók, ha ennek törvényi feltételei biztosítottak. (ADATV_ÖSSZEKAPCS)

A levéltári anyagban előfordulhatnak személyes és különleges személyes adatok (a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó adatok).

Mind a különböző, mind az egyazon iratképzőtől származó levéltári anyag tekintetében biztosítani kell, hogy a különböző adatkezelések, csak akkor legyenek összekapcsolhatók, ha ahhoz az érintett hozzájárul, ha törvény kifejezetten megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Ezt a feltételt egy levéltáron belül őrzött anyagok tekintetében is teljesíteni kell. [Avtv. 8. § (1)]

2.3.7.3. Minden egyes adattovábbítást naplózni kell. (ADATV_NAPLO)

A rendszert úgy kell kialakítani, hogy minden egyes adattovábbítás – különös tekintettel a személyes adatoknak harmadik személyek részére történő hozzáférhetővé tételére - naplózott le-

gyen. A naplózást úgy kell végezni, hogy a naplófájlokból megállapítható legyen a továbbított adat, valamint az, hogy mikor, kik és milyen célból kapták meg az adatokat. Ahhoz, hogy az érintett számára a róla nyilvántartott adatok megismerhetőek és átláthatóak legyenek, az adatkezelő köteles kérésre tájékoztatást adni. A törvénynek megfelelő tájékoztatás része, hogy az érintett személy információhoz jusson arra vonatkozóan, hogy kinek és milyen adatát továbbították. A törvény ezért úgynevezett adattovábbítási nyilvántartás vezetését írja elő, amely nem feltétlenül önálló nyilvántartás, lehet a közlevéltár kutatói nyilvántartásával integrált funkció, mivel a Ltv. alapján „A közlevéltár a kutatásra átadott levéltári anyagról nyilvántartást vezet, és a kutató személyes adatainak védelméről az Avtv. rendelkezései szerint gondoskodik.”. A személyes adatokat is tartalmazó naplófájlokat öt évig, a különleges adatok továbbítására vonatkozó adatokat húsz évig kell megőrizni. A levéltárnak biztosítania kell, hogy az általa kezelt adatok, tekintetében az érintett tájékoztatás kaphasson arról, hogy kik és milyen célból kapják vagy kapták meg a személyes adatait. Az adatokhoz való hozzáférés biztosítását a logfájlok igazolják. Az adattovábbítási nyilvántartásban csak az adatvédelmi törvényben meghatározott céllal és ideig lehet őrizni a közérdekű adatokhoz való hozzáféréssel kapcsolatos személyes adatokat. [Avtv. 12. § (1), 21/A. § (1), Ltv. 22. § (4), EKINT 7-9., PLEDGE CU-0009]

2.3.8. KATASZTRÓFATŰRÉS (KAT)

2.3.8.1. A levéltárnak rendelkeznie kell megfelelő írásos katasztrófa- és visszaállítási tervvel, (KAT_KATTERV)

A levéltárnak írásos tervvel kell rendelkeznie jóváhagyási folyamatokkal, arra az esetre, hogy mi történik meghatározott katasztrófák esetén (tűz, árvíz, rendszer veszélyeztetés stb.) és kinek milyen feladata van ilyen esetben. A katasztrófaterv részletessége és az abban tárgyalt egyes kockázatok összhangban kell, hogy legyenek az elektronikus levéltár elhelyezkedésével és a szolgáltatási szint elvárásaival. A tűz lényegében univerzális kockázat, de a földrengés nem indokol minden földrajzi helyen egyedi katasztrófatervet. A helyi földrajzi, földtani, meteorológiai adatok felhasználhatók a kockázatok értékelésére. A katasztrófatervnek mindazonáltal kezelnie kell nem specifikált helyzeteket is, amelyeknek meghatározott következményei vannak, mint például az épület megközelíthetetlensége. A katasztrófatervnek tartalmaznia kell szolgáltatásfolyamatossági tervet, és a szerepek és a tevékenységek összekapcsolását. [TRAC C3.4, PLEDGE TI-005]

2.3.8.2. Katasztrófahelyzetben a megbízható rendszereknek olyan funkciókat kell nyújtaniuk, melyek az elektronikus levéltárnak lehetővé teszik a működés folytatását, alternatív megbízható rendszerek használatával. (KAT_FOLYT)

A rendelkezésre állásra vonatkozó követelmények nem alkalmazhatók katasztrófahelyzetben. Ilyen esetben a megbízható rendszereknek az elfogadható maximális szolgáltatás kiesésre vo-

natkozó követelményeknek kell megfelelniük. Ez nem jelenti a tartalék helyszínen adott teljes tartalékrendszer-működtetési kötelezettséget. Az adathordozókon tárolt archivált adatok, valamint az adatbázisban tárolt metaadatok vonatkozásában azonban megkövetelik a földrajzilag elkülönült tartalék helyszínen való tárolást. (Így egy katasztrófa esetén is megvan az archivált adatok megőrzési lehetősége.) A tartalék helyszín kijelölésekor alapvető szempont, hogy a két helyszínt reálisan ne veszélyeztessék ugyanazok a környezeti hatások (pl. ne legyen mindkét helyszín ugyanazon folyó mentén). [NHHB SO2.1]

2.3.9. MENTÉS, HELYREÁLLÍTÁS, ELVÁRT REDUNDANCIÁK (MENT)

A mentés és helyreállítás csak azokra a rendszerre és szubjektumokra vonatkozó információkra és egyéb adatokra vonatkozik, melyek a rendszer hibát vagy katasztrófát követő helyreállításhoz szükségesek.

2.3.9.1. Az archívumnak rendelkeznie kell automatikus mentési funkcióval. (MENT_AUTMENT)

A levéltárnak minden körülmények között el kell kerülnie az adatvesztést. Olyan mentési renddel és automatikus biztonsági mentésekkel kell rendelkeznie, amelyek biztosítják, hogy az érintett szolgáltatás működése a biztonsági követelményeknek megfelelő helyreállítási időn belül helyreállítható, az éppen folyamatban lévő eljárás, a biztonsági követelményeknek megfelelő helyreállítási időn belül helyreállítható, folytatható legyen. A biztonsági mentéseknek biztosítaniuk kell azt is, hogy a már lefolytatott eljárások, az adott eljárásra vonatkozó követelmények szerint rekonstruálhatóak legyenek. A szabályzatban rögzített mentési rend meghatározza a mentések típusát, módját, a visszatöltési és helyreállítási tesztek rendjét, valamint a mentési eljárásokat. A mentéseket azok tartalmától függően kockázati szempontból elkülönítetten, az üzemi rendszertől műszakilag független, területileg elkülönülten kell őrizni.

A mentések gyakoriságát a tárolt adatokban bekövetkező változásokhoz (SIP befogadás, migráció, stb.) kell igazítani.

A biztonsági másolatok kezelése során az adatok elhelyezését és tárolását olyan dokumentáltsággal és módon kell végezni, amely a rendszer teljes megsemmisülése esetén is lehetővé teszi a nyilvántartás azonos funkcionalitású, és teljes adattartalmú újbóli rövid idő alatt történő kialakítását.

[223/2009. 16.§, NHHB BK1]

2.3.9.2. A rendszernek biztosítania kell a mentési információ sértetlenségét és bizalmasságát (MENT_INFBIZT)

A biztonsági őrzés során gondoskodni kell arról, hogy az adatokat az arra jogosult személyen kívül más ne ismerhesse meg, valamint biztosítani kell az adatok jogosulatlan személy általi megsemmisítése, megváltoztatása vagy hozzáférhetetlenné tétele elleni védelmét mind a szervezeten belülről, mind a szervezeten kívülről jövő informatikai és más támadások esetén. [NHHB BK2]

2.3.10. AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE (INC)

2.3.10.1. Az elektronikus levéltárnak alkalmaznia kell az információs rendszerekhez kapcsolódó információbiztonsági események és gyenge pontok felismerésének olyan módját, amely lehetővé teszi a helyesbítő tevékenységek időben való megtételét. (INC_FELISM)

A levéltárnak időben és egyeztetett módon kell cselekednie, hogy gyorsan válaszoljon az eseményekre, és korlátozza a biztonság megsértésének hatását. Minden eseményt jelenteni kell az intézkedésre jogosult vezetőnek az előfordulást követő legrövidebb időn belül. Ahol lehetséges, automatizált megoldások alkalmazása javasolt. [MSZ ISO/IEC 27001:2006 A13.1, MSZ ISO/IEC 17799:2006 13.1, NHHE 5.10.1]

2.3.10.2. Az elektronikus levéltárnak garantálnia kell, hogy konzisztens és hatékony megoldásokat alkalmaz az információbiztonsági incidensek kezelésére. (INC_KEZ)

Annak érdekében, hogy az információbiztonsággal összefüggő incidenseket az elektronikus levéltár következetes és hatékony megközelítéssel kezelje, az információbiztonsági incidensekre történő gyors, hatékony és szabályszerű válasz biztosítása érdekében az információbiztonsági szabályzatban rögzíteni kell a vezetői felelősségeket és eljárásokat. Az elektronikus levéltárnak rendelkeznie kell olyan mechanizmusokkal, amelyek lehetővé teszik az információbiztonsági incidensek tanulságai alapján a hibás működések típusainak, mennyiségének és költségének számszerűsítését és figyelemmel kísérését. [MSZ ISO/IEC 27001:2006 A13.2, MSZ ISO/IEC 17799:2006 13.2]

2.4. Közös infrastruktúrát használó elektronikus levéltárak követelményei (KÖZINF)

2.4.1.1. A rendszert úgy kell kialakítani, hogy a különböző levéltárakhoz tartozó információk egymástól legalább logikailag elkülönüljenek. (KOZINF_LOG)

A logikai elkülönülésnek biztosítania kell a levéltári illetékesség fenntartását, vagyis hogy minden levéltár csak a saját adatbázisaihoz és digitális objektumaihoz férhessen csak hozzá, az azok fölötti rendelkezés pedig kizárólag az övé legyen. Az elkülönülésnek biztosítania kell, hogy sem a levéltárak külön-külön, sem az adatfeldolgozó *a levéltárak közreműködése nélkül*, sem harmadik személy ne legyen képes összekapcsolni a levéltárak adatait. Ez a követelmény nem

zárja ki az adatok összekapcsolását *a levéltárak közreműködésével*, így biztosítható az adatok összekapcsolása, amikor arra a jogszabály lehetőséget ad, és az összekapcsolás a levéltárak kifejezett célja. pl. közös keresés illetve használat. [EKINT 4.]

2.4.1.2. A rendszert úgy kell kialakítani, hogy biztosítsa a levéltár számára az adatkezelői felelősségének teljes körű érvényesíthetőségét és az adatkezelés kizárólagosságát. (KÖZINF_ADATKEZ)

Az adatfeldolgozó és a levéltárak egymáshoz való viszonyát úgy kell meghatározni, hogy az adatkezelő és az adatfeldolgozói feladatok és felelősségi körök megfelelően elkülönítettek legyenek. Az adatfeldolgozó kizárólag az adatkezelési műveletekhez kapcsolódó technikai feladatokat végezheti. Az adatfeldolgozó az archívumok megbízása alapján látja el feladatát. A rendszernek biztosítania kell, hogy kizárólag a levéltárak legyenek képesek az adatkezelésre vonatkozó döntések meghozatalára (ideértve az adatfeldolgozó számára adott utasításokat, az adatokon végzett bármely művelet, így például gyűjtés, felvétel, rögzítés, rendszerezés, tárolás, megváltoztatás, felhasználás, továbbítás, nyilvánosságra hozatal, az adatok összehangolása vagy összekapcsolása, törlés, stb.). A rendszert úgy kell kialakítani, hogy egy külső adatfeldolgozó technikailag is csak a levéltár utasításai alapján tehessen bármit az adatokkal. A levéltárak, csak a kezelésük alá tartozó adatokra nézve adhatnak utasításokat az adatfeldolgozónak. [Avtv. 2. § (8-9, 15-16), 4. § 4/A. §, EKINT 1.,6., PLEDGE TI-0010]

2.4.1.3. A rendszert úgy kell kialakítani, hogy az egyes levéltárak feladatainak ellátása a finanszírozás tekintetében is elkülöníthető legyen. (KÖZINF_FIN)

A közös infrastruktúra használata nem jelenti azt, hogy az egyes résztvevők azonos mértékben használják a rendszer erőforrásait. A levéltárak alkalmazott megoldásai, a levéltári anyag megőrzése során a közös infrastruktúra igénybe vett erőforrásai legyenek összhangban a levéltárak feladatainak finanszírozásával, ezért a rendszert úgy kell kialakítani, hogy az egyes levéltárakra jutó költségek valamennyi komponens tekintetében egyértelműen elhatárolhatók legyenek.

3. HIVATKOZÁSOK

- (Baracs et. al. 2003) Baracs Tibor–Cseh Gergő Bendegúz–Körmendy Lajos–Szőke Zoltán–Vánkosné Timár Éva: Az elektronikus iratok levéltári archiválása. Levéltári Szemle 2003. 2. sz.
- (Cost 2000) Stewart Granger - Kelly Russell - Ellis Weinberger: Cost Elements of Digital Preservation Version 4.0 October 2000. http://www.leeds.ac.uk/cedars/colman/costElementsOfDP.doc
- (Cost 2005) Cost of Digital Preservation. The Nationaal Archief. The Hague. 2005. http://www.digitaleduurzaamheid.nl/bibliotheek/docs/CoDPv1.pdf
- (CRL 2007) CRL/OCLC/NESTOR/DCC/DPE "Core Requirements for Digital Archives", http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re , (January 2007)
- (DRAMBORA) Digital Curation Centre & DigitalPreservationEurope, Digital Repository Audit Method Based on Risk Assessment (DRAMBORA), Version 1.0, http://www.repositoryaudit.eu/ , (March 2007);
- (Duranti 1995) Duranti, Luciana: Reliability and Authenticity: The Concepts and their Implications." Archivaria 39 (Spring 1995): 5-10
- (EKINT 2009) Adatvédelmi követelmények az e-levéltár projekthez. Eötvös Károly Intézet. 2009. Kézirat.
- (Handbuch) nestor Handbuch: Eine kleine Enzyklopädie der digitalen Langzeitarchivierung hg. v. H. Neuroth, A. Oßwald, R. Scheffel, S. Strathmann, M. Jehn im Rahmen des Projektes: nestor – Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen für Deutschland. Verlag Werner Hülsbusch, Boizenburg, 2009. http://nbn-resolving.de/urn/resolver.pl?urn=urn:nbn:de:0008-2009073109
- (InterPares) Report of the “Authenticity Task Force”. The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project, 2004. http://www.interpares.org/book/interpares_book_d_part1.pdf
- (Jakab 1877) Jakab Elek: A levéltárakról tekintettel a magyar államlevéltár ügyre. Budapest, 1877.
- (Muller, Feith, and Fruin 1968) S. Muller, J.A. Feith and R. Fruin: Manual for the arrangement and description of archives : drawn up by direction of the Netherlands Association of Archivists. New York, 1968.

- (Nestor 2006) nestor Working Group, Catalogue of Criteria for Trusted Digital Repositories , Version 1 (draft for public comment), http://www.nbn-resolving.de/?urn:nbn:de:0008-2006060703 , 2006.
- (NHHB) Biztonsági követelmények elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható rendszereire. Nemzeti Hírközlési Hatóság Hivatala 2007. június
- (NHHE) Eljárásrendi követelmények elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható rendszereire. Nemzeti Hírközlési Hatóság Hivatala 2007. június
- (OAIS 2002) CCSDS (Consultative Committee for Space Data Systems (2002): Reference Model for an Open Archival Information System (OAIS). Blue Book. URL: http://www.ccsds.org/docu/dscgi/ds.py/Get/File-143/650x0b1.pdf
- (PAIMAS 2004) CCSDS (2004): Producer-Archive Interface Methodology - Abstract Standard, Blue Book. URL: http://public.ccsds.org/publications/archive/651x0b1.pdf
- (PLEDGE) Robert Wolfe: PLEDGE POLICY LIST, PLEDGE Project Report,MIT Libraries, 2007. http://pledge.mit.edu/index.php/Main_Page
- (RLG/OCLC 2002) Working Group on Digital Archive Attributes, Trusted Digital Repositories: Attributes and Responsibilities, http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf , (May 2002)
- (Ross és McHugh 2005) Ross, Seamus and Andrew McHugh. 15 October 2005. “Audit and Certification of Digital Repositories: Creating a Mandate for the Digital Curation Centre (DCC).” RLG DigiNews 9:5. www.rlg.org/en/page.php?Page_ID=20793#article1
- (Rothenberg 1999) Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation 1999. http://www.clir.org/pubs/reports/rothenberg/contents.html
- (Spezifikation SIP) SpezifikationSubmission Information Package(SIP). Bundesarchiv. 2009.
- (Székely 2005) Székely Iván: Az elektronikus adatállományok közép- és hosszú távú archiválása. In: IT3 Tanulmányok. 2. kötet. 131-138. Budapest, 2005.
- (TDR 2002) Trusted Digital Repositories: Attributes and Responsibilities. May 2002. Mountain View, CA: RLG. www.rlg.org/en/pdfs/repositories.pdf
- (Ten principles) DCC/DPE/CRL/Nestor: Ten basic characteristics of digital preservation repositories. http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re

- (Todd 2009) Todd, Malcolm: Technology Watch Report File formats for preservation Digital Preservation Coalition. 2009. http://www.dpconline.org/newsroom/file-formats-for-preservation-technology-watch-report.html
- (TRAC 2007) Center for Research Libraries and RLG OCLC Programs, Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist, Version 1.0, http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=91 (February 2007);

4. FÜGGELÉK 1. – FOGALMAK

AIP →Archív Információs Csomag
Archív Információs Csomag [Archival Information Package (AIP)] Az OAIS szabvány által definiált digitális objektum a levéltári megőrzésre.
archívum az elektronikus levéltári funkcionalitás tárolással összefüggő szolgáltatásai
Benyújtott Információs Csomag [Submission Information Package (SIP)] Az OAIS szabvány által definiált entitás a levéltári átadásra.
DIP →Kibocsátott Információs Csomag
elektronikus levéltár A →levéltár által megvalósított, a maradandó értékű iratok megőrzését megvalósító *funkció*.
Kibocsátott Információs Csomag [Dissemination Information Package (DIP)] Az OAIS szabvány által definiált entitás a levéltári anyag használatára.
Hivatali Kapu A →központi rendszer azon pontja, amelyen keresztül a csatlakozott szervezet hozzáfér a központi rendszer által részére biztosított szolgáltatásokhoz, és megfelel a közhasznúság követelményeinek Ekt 2.§
közlevéltár a nem selejtezhető köziratokkal kapcsolatos levéltári feladatokat - ideértve a tudományos és igazgatási feladatokat is - végző, közfeladatot ellátó szerv által fenntartott levéltár
Központi Elektronikus Szolgáltató Rendszer (KR) →központi rendszer
központi rendszer (Központi Elektronikus Szolgáltató Rendszer) az elektronikus közszolgáltatások nyújtását, illetve igénybevételét támogató központi informatikai és kommunikációs rendszerek együttese Ekt 2.§.
levéltár a maradandó értékű iratok tartós megőrzésének, levéltári feldolgozásának és rendeltetésszerű használatának biztosítása céljából létesített intézmény. Ltv. 3.§.
levéltárhasználók A levéltár anyagát felhasználók azonosított csoportja, amelynek tagjai képesek értelmezni egy meghatározott információ halmazt. A levéltárhasználók több felhasználói csoportot is jelenthetnek. (OAIS 2002 1-11.o.)
OAIS

→Open Archival Information System
Open Archival Information System A Consultative Committee for Space Data Systems (CCSDS) által 2001-ben fejlesztett referenciamodell az elektronikus információ hosszú távú megőrzésének modellezésére, amelyet a Nemzetközi Szabványügyi Szervezet ISO 14721:2003 számú szabványként jegyzett be.
SIP →Benyújtott Információs Csomag
Ügyfélkapu Az az eszköz, amely biztosítja, hogy az ügyfél egyedileg azonosított módon biztonságosan léphessen kapcsolatba a központi rendszer útján az elektronikus ügyintézést, illetve elektronikus szolgáltatást nyújtó szervekkel.

5. FÜGGELÉK 2. – A KÖVETELMÉNYEK TELJESÍTÉSE AZ ELEKTRONIKUS LEVÉLTÁR PROJEKT KONZORCIUMI PARTNEREIRE VONATKOZÓAN

Szervezeti és folyamat-követelmények	KD	MOL	BFL
SZK_CEL		☑	☑
SZK_JOGSZ	☑	☑	☑
SZK_SZABV		☑	☑
SZK_KIV		☑	☑
IR_STRAT		☑	☑
IR_TAN		☑	☑
SZERV_STRUKT		☑	☑
SZERV_SZEREP		☑	☑
SZERV_SZETV		☑	☑
SZERV_FELEL		☑	☑
SZERV_LETSZ		☑	☑
SZERV_KEPZ		☑	☑
KSZ_SZAB		☑	☑
KSZ_FELH		☑	☑
KSZ_ELETCIKLUSDOK		☑	☑
KSZ_ATL		☑	☑
KSZ_INT		☑	☑
KSZ_SZERZ		☑	☑

KSZ_SZERZOIJOG		☑	☑
KSZ_VALTKOV		☑	☑
FENNT_FIN	☑	☑	☑
FENNT_VISSZAJ		☑	☑
FENNT_ERT		☑	☑

DIGITÁLIS TARTALOMKEZELÉS	KD	MOL	BFL
BEF_DIGIOBJ		☑	☑
BEF_ELOK		☑	☑
[BEF_ISZ]		☑	☑
BEF_FORRASELL		☑	☑
BEF_TELJELL		☑	☑
BEF_FIZKONTROLL		☑	☑
BEF_VISSZAIG		☑	☑
BEF_SIPBEF.		☑	☑
BEF_BEAV.		☑	☑
BEF_AIPDEF		☑	☑
BEF_SIPAIP		☑	☑
BEF_SIPALLAPOT		☑	☑
BEF_AIPAZON		☑	☑
BEF_ERTINF		☑	☑

BEF_PDI		☑	☑
BEF_ERTELMEZ		☑	☑
BEF_AIPELLENORZES		☑	☑
BEF_INTEGR		☑	☑
BEF_ADMINFMETAADAT		☑	☑
MOT_MEGORZSTRAT		☑	☑
MOT_FORMATUM		☑	☑
MOT_METAADAT		☑	☑
MOT_MEGORZOTTTUL		☑	☑
MOT_RIELEVULES		☑	☑
TAR_AIPINTEGR	☑		
TAR_ARCHINTEGR	☑		
TAR_AIPOLV	☑		
ADATK_VEGYESIR		☑	☑
ADATK_MAKOZZETETEL		☑	☑
ADATK_MAROGZITES		☑	☑
ADATK_MAHIVINT		☑	☑
FELD_TARTMEGORZ		☑	☑
FELD_MIGR		☑	☑
FELD_BEAVROGZ		☑	☑
FELD_VEGY		☑	☑
FELD_TÖRL	☑	☑	☑

HASZN_KUTSZAB		☑	☑
HASZN_FELHCSOP		☑	☑
HASZN_DIGOBJINF		☑	☑
HASZN_HOZZAFBIZT		☑	☑
HASZN_ERTELM		☑	☑
HASZN_NAPLOZAS	☑	☑	☑
HASZN_JOGOSULTSAG	☑	☑	☑
HASZN_FELHAZON	☑	☑	☑
HASZN_DIGIOBJOSSZ		☑	☑
HASZN_OSSZESKERES		☑	☑
HASZN_MASOLAT		☑	☑

Műszaki és biztonsági követelmények	KD	MOL	BFL
INF_HWSW	☑	☑	☑
INF_IOP	☑	☑	☑
INF_KAPACITAS	☑	☑	☑
INF_PELDANYOK	☑	☑	☑
INF_SZINKRON	☑		
INF_ADATVESZTES	☑		
INF_ADATVESZTDOK	☑		
INF_HARDVERCSERE	☑		

INF_KRITRSZ	☑		
KOCK_EL		☑	☑
INFBIZT_IBSZ	☑	☑	☑
INFBIZT_ELL	☑	☑	☑
FIZB_HOZZ	☑	☑	☑
FIZB_BER	☑	☑	☑
AZON_KIKENYSZERIT	☑	☑	☑
AZON_SIKERTELEN	☑	☑	☑
HOZZ_RENDSZFUNKC	☑	☑	☑
HOZZ_SZEREPKOR	☑	☑	☑
ADATV_SZEMADAT	☑	☑	☑
ADATV_NAPLO	☑	☑	☑
ADATV_ÖSSZEKAPCS	☑	☑	☑
KAT_KATTERV	☑	☑	☑
KAT_FOLYT	☑	☑	☑
MENT_AUTMENT	☑		
MENT_INFBIZT	☑		
INC_FELISM	☑	☑	☑
INC_KEZ	☑	☑	☑

Közös infrastruktúra követelményei	KD	MOL	BFL
KOZINF_LOG		☑	☑
KOZINF_ADATKEZ		☑	☑
KOZINF_FIN	☑	☑	☑