



## A NÓGRÁD VÁRMEGYEI SZAKKÉPZÉSI CENTRUM Archiválási szabályzat

Jóváhagyta: .....(Gembiczki Ferenc) kancellár

Jóváhagyta: .....(Baranyi Zoltán) főigazgató

Hatályos: 2025.03.31-től

Érvényes visszavonásig



A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (továbbiakban: Dáptv.), a digitális állampolgárság egyes szabályairól szóló 321/2024. (XI.6.) Korm. rendelet, valamint a digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről szóló 322/2024. (XI.6.) Korm. rendelet előírásainak figyelembe vételével, a Nógrád Vármegyei Szakképzési Centrum Szervezeti és Működési Szabályzatában biztosított jogkörömben eljárva a Nógrád Vármegyei Szakképzési Centrum informatikai rendszereinek és információvagyonának mentésére, archiválására vonatkozó feladatokat, kötelezettségeket az alábbiak szerint szabályozom.

## **Általános rendelkezések**

### **A szabályzat alkalmazási területe**

A Szabályzat célja, hogy meghatározza a Nógrád Vármegyei Szakképzési Centrum (a továbbiakban: Centrum) Dáptv. 39. § (7) bekezdése szerint, az ügyek intézésével kapcsolatos elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentésével és adattrezor szolgáltatást nyújtó őrző szervhez továbbításával, valamint a kapcsolódó folyamatokkal kapcsolatos részletszabályokat.

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

### **A szabályzat személyi hatálya**

A szabályzat személyi hatálya kiterjed a Centrumra, mint adatkezelőre, a Centrum belső információs rendszereit üzemeltető szervezeti egységekre, a kancellárra, a főigazgatóra, a gazdasági vezetőre, a szakmai igazgatóhelyettesre, munkavállalóra, munkavégzésre irányuló egyéb jogviszony alapján a Centrum által foglalkoztatott személyekre, valamint az üzemeltetésben a Centrum általi mentési archiválási folyamatban résztvevő, illetve azt szerződés alapján végző harmadik személyre.

### **A szabályzat tárgyi hatálya**

A Szabályzat tárgyi hatálya a digitális szolgáltatás részét képező vagy a digitális szolgáltatás nyújtásával, intézésével kapcsolatos, elektronikus információs rendszereihez és nyilvántartásaihoz szervesen kapcsolódó minden, a Centrum által üzemeltetett informatikai rendszer (hardver, operációs rendszer, alkalmazás szerver, alkalmazás, adatbázis szerver, adatbázis, web szerver, file szerver, dokumentum kezelő) kiterjed.

### **A szabályzat időbeli hatálya**

A szabályzat az aláírás dátumával lép hatályba és visszavonásig, verzióváltásig marad hatályban.

### **Kapcsolódó szabályzatok, eljárások, rendelkezések**

A szabályzat rendelkezéseit a digitális szolgáltatás részét képező vagy ahhoz szervesen kapcsolódó minden informatikai rendszer esetében a szabályzatban részletezett módon teljeskörűen alkalmazni kell. Az adattrezor archiválási kötelezettség a Centrumnál, mint digitális szolgáltatást biztosító szervet terheli az általa saját szoftverkörnyezetben kezelt elektronikus információk rendszereiben és a nyilvántartásaiban tárolt nem minősített adatok tekintetében, vagy azokkal együtt teljes futtatási környezet tekintetében. A Centrum Cégháló rendszerei a KRÉTA POSZEIDON Irat- és dokumentumkezelő rendszerbe nincsenek bekötve, az elektronikus úton érkező és ott kiküldött küldemények archiválási és trezorálási feladatait is el kell látni. A hivatali kapun, céghálón érkező adatokat úgy szükséges archiválni, hogy az adatokból az eredeti környezet teljes vagy részleges megsemmisülése esetén helyreállítható legyen az eredeti működés a megfelelő hardvereszközök üzembe helyezését követően.

A digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről szóló 322/2024. (XI.6.) Korm. rendelet szerint a Centrum a digitális szolgáltatás biztosításához szükséges elektronikus információk rendszerei a 4. függelékben jelölt archiválási osztályba tartoznak, melyek archiválását az ott meghatározott gyakorisággal kell elvégezni.

A szabályzat során alkalmazandó jogszabályok köre:

- a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény,
- a digitális állampolgárság egyes szabályairól szóló 321/2024. (XI.6.) Korm. rendelet,
- digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről szóló 322/2024. (XI.6.) Korm. rendelet.

## Értelmező rendelkezések

A szabályzat értelmében:

**Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

**Adatfeldolgozó:** az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

**Adatkezelés:** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok

további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.

**Adatkezelő:** az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja.

**Adattrezor-archiválás:** a Dáptv. 39. § (7) bekezdése szerinti, a digitális szolgáltatást biztosító szervezeteknek a digitális szolgáltatások nyújtásával, intézésével kapcsolatos, elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentése.

**Archiválás:** a nem, vagy nagyon ritkán használt, de megőrzendő adatok áthelyezése a feldolgozó rendszer tárolójáról egy másik elkülönített tárolóra.

**BCP (business continuity planning):** működés folytonossági terv.

**DRP (data recovery planning):** adat helyreállítási terv.

**EIR (elektronikus információs rendszer):** az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók) és szoftverek együttese.

**Inkrementális mentés:** nem kerül elmentésre minden kiválasztott elem, csak azok, amelyek a korábbi mentés óta változtak. Két alapvető típusa:

- a.) A **kumulatív mentés** során mindig az utolsó teljes mentés óta megváltozott adategységek kerülnek elmentésre.
- b.) A **differenciális mentés** során csak az utolsó inkrementális mentés óta megváltozott adategységek kerülnek elmentésre.

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

**Kockázatelemzés:** az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjának), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

**Kormányzati adattrezor:** olyan kormányzati adatbank, amely az adattrezor archivált állományokat fogadja és biztonságosan tárolj, őrzi és az adatok adatkezelő részére történő kiadásával újraépíthetővé teszi a különböző informatikai rendszereket.

**Központi mentés:** alapértelmezésben a mentések a rendszerbe állított központi mentőeszköz igénybevételel történnek.

**Központi mentési eszköz:** a szervezet adatbázisainak, alkalmazásainak, operációs rendszereinek és ezek környezeti mentési igényeinek végrehajtására rendszerbe állított

nagyteljesítményű, megfelelő biztonsági megoldással és menedzsment felülettel rendelkező berendezés.

**Offline mentés:** a mentés a szolgáltatások leállításával történik, a szolgáltatások a mentés ideje alatt nem érhetőek el.

**Online mentés:** a mentés online módon, az informatikai szolgáltatás leállítása nélkül történik. A mentés ideje alatt az adott szolgáltatás elérhető, azonban lehetnek olyan funkciók, amelyek a mentés ideje alatt nem, vagy csak korlátozott mértékben vehetők igénybe.

**Tartós adathordozó:** olyan eszköz, amely a címzett számára lehetővé teszi a neki címzett adatoknak az adat céljának megfelelő ideig történő tartós tárolását és a tárolt adatok változatlan formában és tartalommal történő megjelenítését. Ilyen eszköz különösen az USB kulcs, a CD-ROM, a DVD, a memória kártya, a számítógép merevlemeze.

**Teljes (full) mentés:** minden kiválasztott elem mentésre kerül.

**Teljes körű védelem:** az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

**Visszaállítás:** meghibásodás vagy sérülés miatt leállt informatikai szolgáltatás helyreállítása, amely megkívánhatja a rendszerek és adatbázisok mentéseinek visszatöltését. Katasztrófa-elhárítás esetén leginkább a gyors, ideiglenes szolgáltatás visszaállítást jelenti, megkülönböztetve a végleges helyreállítástól.

**Zárt védelem:** az összes számításba vehető fenyegetést figyelembe vevő védelem.

## Archiválás

### Az archiválási folyamat résztvevői

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve a programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával, valamint a Centrum feladatellátási ciklusával. A Centrum által használt Cégekportal archiválási folyamatát a NISZ Zrt. végzi, az egyéb elektronikus információs rendszerek (EIR) archiválási folyamatát pedig a Nemzeti Felnőttképzési és Szakképzési Hivatal biztosítja.

### Kockázatelemzés

A Centrum meghatározza az ügymenet folytonosság biztosításához szükséges szabályokat, követelményeket, amelynek érdekében:

- elkészíti a működés szempontjából jelentős informatikai szolgáltatások helyreállítási terveit
- a fontos informatikai szolgáltatások meghatározásához kockázatelemzést végez,
- az azonosított szolgáltatásoknál:
  - megvizsgálja a kulcsfontosságú elemeket,

- meghatározza a még tolerálható helyreállítási időket,
- elkészíti a helyreállítási terveket,
- azokat a gyakorlatban is teszteli.

A szabályokat és követelményeket tartalmazó dokumentumok előkészítését és kockázatelemzést a Centrum informatikusai és az integrált kockázatkezelési rendszer koordinálására kijelölt szervezeti felelős végzi el.

### ***Internet kapcsolat (WAN) kiesése***

Működésfolytonosság (BCP)

Hatása az ügymenetre: kritikus (nem érhető el a központi szerver)

Valószínűsége: magas rendelkezésre állás miatt évente 1 alkalom

Helyreállítási idő: legfeljebb 12 óra

Kockázatkezelés:

Az esetet a szolgáltatónál be kell jelenteni.

Helyreállítás (DRP):

Fővonal hiba esetén: az esetet a szolgáltatónak haladéktalanul be kell jelenteni

Router / modem hiba esetén: funkcionális csereeszköz haladéktalan igénylése a szolgáltatónál.

### ***Belső hálózat (LAN) elemeinek meghibásodása***

Működésfolytonosság (BCP)

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

Valószínűsége: évente 1 alkalom

Helyreállítási idő: legfeljebb 4 óra

Kockázatkezelés:

Jó minőségű hálózati eszközök és kábelezés alkalmazása, hálózati szolgáltató bevonása magas SLA-val. Rendszeres karbantartással, teszteléssel jelentősen csökkenthető a meghibásodás valószínűsége. Meghibásodás esetén a hibás eszközök azonnali cseréje.

Helyreállítás (DRP):

Aktív elemek meghibásodása esetén:

- hibabehatárolás,
- a hiba jelentése a szolgáltatónak,
- funkcionális csereeszköz leszállítása, beállítása és konfigurálása,
- tesztelés,
- próbaüzem,
- éles üzem,
- dokumentálás.

Passzív elem (kábel, rack stb.) meghibásodása esetén:

- hibabehatárolás,
- a hiba jelentése, az érintettek tájékoztatása,
- passzív szakasz, vagy alkatrész cseréje,
- tesztelés,
- dokumentálás.

### **Csoportmunka szerver meghibásodása**

Működésfolytonosság (BCP)

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

Valószínűsége: háromévente 1 alkalom

Helyreállítási idő: kb. 16 óra

#### **Kockázatkezelés:**

Karbantartási szerződés a szerver szállítójával. Jó minőségű alkatrészek alkalmazása, a bizonytalanok cseréje, megfelelő szintű adattárolás biztosítása. Adatbázis és fájlstruktúra mentése napi gyakorisággal. Rendszernapló állományok folyamatos mentése, elemzése és dokumentálása. Meghibásodás esetén a hibás alkatrész azonnali cseréje, újratelepítés, adatbázis betöltés, tesztelés és üzembe helyezés.

#### **Helyreállítás (DRP):**

Alkatrész (alaplap, CPU, memória, HDD, táp) meghibásodása esetén:

- hibabehatárolás,
- a hiba jelentése a szolgáltatónak, kancellár tájékoztatása,
- adatok másolása egy másik eszközön,
- hibátlanak gondolt elemek tesztelése egy működő környezetben,
- csere alkatrészek beépítése, pótlása
- konfigurálás,
- tesztelés,
- szükség esetén az adatok visszamásolása,
- próbaüzem,
- éles üzem.

### **Az archiválás folyamata**

A mentési, archiválási rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell annak érdekében, hogy minimalizálni lehessen az emberi tényezőtől adódó hibák előfordulásának valószínűségét. A mentéseknek ki kell terjednie a működési folyamatok és tevékenységek támogatásában és kiszolgálásában részt vevő informatikai eszközökre, illetve azok elhelyezésére szolgáló kiszolgáló rendszerekre, infrastruktúrára. Megfelelő gyakorisággal gondoskodni kell az EIR rendszerek mentéséről, a mentések tárolása fizikailag biztonságos legyen. A Nógrád Vármegyei Szakképzési Centrum az EIR rendszerek mentéséről külön nem gondoskodik, az ezzel kapcsolatos hatáskörrel a középírányító szerv – a Nemzeti Szakképzési és Felnőttképzési Hivatal – rendelkezik. Védni kell illetéktelen hozzáféréstől, fizikai behatásoktól (tűz, víz, mágnesesség).

A központi szerveren tárolt elektronikus információvagyon a biztonsági káresemények ellen szintén mentéssel kell védeni. A mentéseket minden mentési rendet érintő (fizikai, logikai, adminisztratív) változáskor, de legalább évente egyszer ellenőrizni kell. Az ellenőrzéseket dokumentált módon kell végrehajtani. A mentéseket a szerverektől elkülönítve, legalább külön helyiségben kell tárolni, védve mind a különböző fizikai káreseményektől (tűz, vízbetörés stb.), mind az illetéktelen hozzáféréstől (lopás, illegális másolás).

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

Az adattrezor archiválást titkosító kulcs alkalmazásával az adatfeldolgozó úgy végzi, hogy abból az adatkezelőnél működtetett elektronikus információs rendszerek visszaállíthatók legyenek. Az adatfeldolgozónak jól beazonosítható módon meg kell jelölnie, hogy az átadott adatállomány mely adatkezelő elektronikus információs rendszer archiválást tartalmazza. Az adattrezor archiválásnak tartalmaznia kell a visszaállításhoz szükséges dokumentációt. Az őrzésért felelős szervnek átadásra kerülő adatállománynak a technikai archiváláskori állása szerint rosszindulatú szoftverködtől való mentessége az adatfeldolgozó felelőssége.

Az archiválás folyamat főbb szakaszai:

- a) az üzemeltető végzi az érintett adatállomány kijelölését és mentését az adatmennyiségtől függő típusú adathordozóra, illetve annak ellenőrzését,
- b) az üzemeltető végzi a mentett adatokat tartalmazó adathordozó titkosítását,
- c) az adathordozó átvétele és szállítása.

### **Archiválás dokumentálása**

Az archiválás naplózása gépi alapú. A titkosított mentési állomány mellé egy titkosítatlan szöveg fájlt kell elkészíteni, amely a mentett állományok felsorolását tartalmazza. A szöveg fájl megőrzési ideje megegyezik a vonatkozó mentési állomány megőrzési idejével. A mentési média típusa: elektronikus adathordozó.

### **A tárolt és mentésre kerülő adatok köre**

A Cégek kapun keresztül érkezett és onnan küldött küldemények manuálisan kerülnek le- és feltöltésére, a manuálisan iktatott küldemények elektronikus iktatására és az elektronikusan tárolt dokumentumok nyilvántartására az iratkezelő szoftver szolgál. A Cégek kapu archiválási folyamatát a NISZ Zrt. látja el.

### **Tesztelés**

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

A biztonsági mentést végző szolgáltató beszámoltatható a biztonsági mentésről arra vonatkozóan, hogy hitelt érdemlően igazolja az archivált és mentett adatállományból az eredeti

állapot helyreállíthatóságát a biztonsági mentési állományok, illetve archivált állományok alapján. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

#### **Az archiválási szabályzat módosítása**

Az archiválási szabályzatot, a benne foglalt információk változása esetén, a változást követő 3 napon belül frissíteni kell.

#### **Az archiválási szabályzat felülvizsgálata**

Az archiválási szabályzatot annak elkészítésekor, valamint a módosított archiválási szabályzat egységes szerkezetű változatát az archiválási szabályzat módosításakor a Felügyeletnek meg kell küldeni. Hivatali kapu cím: EUF, KRID: 524741381.

A Felügyelet az archiválási szabályzat beérkezését követő 60 napon belül azt felülvizsgálja.

#### **Az adattrezor-archiválás ellenőrzése**

Az archiválás ellenőrzésére az Elektronikus Ügyintézési Felügyelet jogosult.

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

### **Záró rendelkezések**

A szabályzat 2025. március 31-én lép hatályba. A szabályzatot évente, illetve jelentősebb infrastrukturális változás, jogszabályváltozás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell, melyért a kancellár a felelős.

A szabályzatot és módosításait az Elektronikus Ügyintézési Felügyelet részére meg kell küldeni.

A szabályzat megismertetése A Nógrád Vármegyei Szakképzési Centrum Belső Kontrollrendszer Szabályzatának megfelelően a Nógrád Vármegyei Szakképzési Centrum hivatalos honlapján történő közzététellel történik.

Salgótarján, 2025. március 31.

  
Gembiczki Ferenc  
kancellár



  
Baranyi Zoltán  
főigazgató

**A 2023.03.31-étől hatályos NSZFH/630/001800-1/2025 számú  
szabályzat 1.számú függelékének a szabályzat kiadásakor, 2025.03.31-  
től hatályos változata**


**PSZD archiválási osztály elemzési tábla**

<b>Az EIR-hez tartozó alapadatok 3.0</b>	
Elektronikus Információs Rendszer neve:	---
EIR rövid kódja:	---
EIR állapota:	---
Adatkezelő szervezet:	
Adatfeldolgozó szervezet:	
Mentési osztályba sorolás dátuma:	
EÜF kapcsolattartó megnevezése:	
EÜF kapcsolattartó elérhetősége:	
Egy teljes mentés mérete (Mbyte):	
EIR rövid leírása:	
<b>Archiválási kategória meghatározása</b>	
EIR archiválási osztály	
EIR archiválásának módja	

Salgótarján, 2025. március 31.

  
Gembiczki Ferenc  
kancellár



  
Baranyi Zoltán  
főigazgató

**A 2023.03.31-étől hatályos NSZFH/630/0011799-1/2025 számú  
szabályzat 2.számú függelékének a szabályzat kiadásakor, 2025.03.31-  
től hatályos változata**

<b>Archiválási osztályba sorolás összesítő táblázat</b>							
<b>Adatkezelő szervezet:</b>		<b>Nógrád Vármegyei Szakképzési Centrum</b>					
<b>Ssz.</b>	<b>Elektronikus Információs Rendszer neve</b>	<b>EIR rövid kódja</b>	<b>EIR állapota</b>	<b>Adatfeldolgozó szervezet megnevezése</b>	<b>Mentési osztályba sorolás dátuma</b>	<b>EÜF kapcsolattartó megnevezése</b>	<b>EÜF kapcsolattartó elérhetősége</b>
1.	---						

Salgótarján, 2025. március 31.

  
Gembiczki Ferenc  
kancellár

  
Baranyi Zoltán  
főigazgató



