Saint James Eye Clinic Kft.

MÁSOLATKÉSZÍTÉSI SZABÁLYZATA

Verzió: 1.0

2025.11.26

A Szabályzatot jóváhagyta:

……..

Saint James Eye Clinic Kft.

Verziókövetés:

Verzió	Módosítás tartalma	Hatálybalépés
1.0	Másolatkészítési szabályzat 1.0	2025.12.01

1 **Tartalomjegyzék**

Tartalomjegyzék

2 CÉG AZONOSÍTÓ ADATAI 3

3 A SZABÁLYZAT CÉLJA 3

4 FOGALMAK 3

5 SZABÁLYZAT HATÁLYA 4

6 A MÁSOLAT KÉSZÍTÉS FOLYAMATA 4

6.1 DocIT elektronikus irattári rendszer 4

6.2 A szabályzat hatálya, hitelesítendő iratok köre 4

6.3 A másolatkészítés és validálás szabályai 5

6.4 Hiteles másolatkészítés, hitelesítési eljárás 6

6.5 Az eredeti papír alapú iratok további sorsa 6

6.6 Másolatok hitelességének ellenőrzése 7

6.7 Elektronikus másolatok archiválása 7

7 EGYÉB RENDELKEZÉSEK 7

8 JOGSZABÁLYI MEGFELELŐSÉG 8

1. számú melléklet *:* Hiteles elektronikus másolat készítésére és validálására és hitelesítésre feljogosított személyek 9

2. számú melléklet: MŰSZAKI DOKUMENTÁCIÓ 10

2 CÉG AZONOSÍTÓ ADATAI

Cég megnevezése: Saint James Eye Clinic Kft.
Székhely: 1034 Budapest Bécsi út 68-84
Adószám: 32723834-2-41
Webhely: https://www.lassjol.hu
Telefonszám: 06/1 788 2927

3 A SZABÁLYZAT CÉLJA

a Saint James Eye Clinic Kft. megvalósítja meghatározott típusú papíralapú iratainak hiteles elektronikus irattá történő átalakítását, a vonatkozó alapvető és egységes szabályok meghatározása 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 (a továbbiakban: Korm. rendelet), valamint a digitális archiválás szabályairól szóló 1/2018. (VI.29.) ITM rendelet figyelembevételével.
A másolatkészítés célja, hogy a papír alapú iratokról hiteles elektronikus másolat készüljön, ezzel a papír alapú iratok fizikai megőrzése mellőzhető legyen.

a Saint James Eye Clinic Kft. iratainak digitalizálásához és azokról történő hiteles másolat készítés hez külső szolgáltatót vesz igénybe.
A megbízott szolgáltató, a DWS Digital Kft. , ügyfelei részére végzett hiteles másolatkészítést szolgáltatás nyújtás keretében végzi, melynek igénybevételére a felek között megkötött szerződés, a szolgáltatási részleteket és a biztonsági követelményeket rendező megállapodás alapján valósul meg (továbbiakban: Szolgáltatás).
Jelen másolatkészítési rend részletezi a másolatkészítés szervezeti kereteit, valamint a másolatkészítési folyamat során teljesített jogszabályi és műszaki követelményeket.

4 FOGALMAK

A Szabályzat vonatkozásában:
Papíralapú dokumentum: a papíron rögzített minden olyan szöveg, számadatsor, térkép, tervrajz, vázlat, kép vagy más adat, amely bármely eszköz felhasználásával és bármely eljárással keletkezett;
Hiteles elektronikus másolat: valamely nem elektronikus dokumentumról a 321/2024. (XI.6.) Korm. rendelet rendelkezései szerint készült, azzal képileg vagy tartalmilag egyező, joghatás kiváltására alkalmas, elektronikus eszköz útján értelmezhető adategyüttes.
Hitelesítési záradék: „Az eredeti papíralapú dokumentummal egyező” valamint “Automatikus másolatkészítés” szöveggel és az 321/2024. (XI.6.) Korm. rendelet szerinti adattartalommal elkészített állomány, amely az elektronikus másolat elválaszthatatlan részét képezi.
Automatikus másolatkészítés: másolatkészítés külső beavatkozástól mentes zárt rendszerben történik.
Képi megfelelés: az elektronikus másolat azon tulajdonsága, amely biztosítja a papíralapú dokumentum – joghatás kiváltása szempontjából lényeges – tartalmi és formai elemeinek megismerhetőségét;
Tartalmi megfelelés: az elektronikus másolat azon tulajdonsága, amely szerint az – a hozzá kapcsolódó metaadatokkal együttesen – biztosítja a papíralapú dokumentum joghatás kiváltása szempontjából lényeges tartalmi elemeinek megismerhetőségét, de nem biztosítja a képi megfelelést;
Másolatkészítő rendszer: a másolatkészítés során alkalmazott hardver, szoftver, humánerőforrás, jelen Szabályzat, valamint ezek együttese;

Metaadat: a tárolt dokumentumot leíró ismertető adatok.
Digitalizálás: Olyan eljárás, amely az analóg felépítésű információt számítástechnikai eszközök számára feldolgozható, digitális információvá alakítja át.

5 SZABÁLYZAT HATÁLYA

A Másolatkészítési Szabályzat (továbbiakban Szabályzat) tárgyi hatálya kiterjed a másolatkészítést megvalósító teljes informatikai rendszerre: számítástechnikai eszközökre, szoftverekre, az informatikai rendszer fizikai környezetére. A Szabályzat személyi hatálya kiterjed mindazon személyekre, akik a másolatkészítési eljárásban részt vesznek. A folyamatban definiált szerepköröket és résztvevőket a Szabályzat 1. sz. melléklete tartalmazza.
A Szabályzat időbeli hatálya annak kiadásától a módosításig, vagy visszavonásig érvényes.

6 A MÁSOLAT KÉSZÍTÉS FOLYAMATA

6.1 DocIT elektronikus irattári rendszer

A DWS Digital Kft. , mint iratfeldolgozó, hiteles másolatkészítési szolgáltatási tevékenységét saját, felhő alapú DocIT rendszerével valósítja meg.
DWS a feldolgozás időtartamára biztosítja az elektronikus irattár szolgáltatást: a http://szemklinika.docit.hu honlap és annak valamennyi URL alatt elérhető funkciójának (a továbbiakban együttesen: DocIT) használatát.
A DocIT rendszer eszközfüggetlen, reszponzív, web alapú alkalmazás, melynek köszönhetően az iratok, dokumentumok kezelése, visszakeresése, hitelesítése a program telepítése nélkül bármilyen eszközről, internet böngésző alkalmazással megvalósítható. A DocIT rendszerhez a hozzáférés felhasználói regisztrációhoz kötött, irattípushoz, mappához rendelt többszintű (keresés, adatmódosítás, letöltés, törlés) jogosultság biztosítása mellett.

DWS Digital Kft. végzi a Saint James Eye Clinic Kft. iratainak nagytömegű szkennelését és az elektronikus formában rendelkezésre álló fájlok feltöltését az elektronikus irattárba, DocIT rendszerbe, valamint a visszakeresést biztosító adatok rögzítését, továbbá a jelen szabályzat részét képező validálást és hitelesítést. DWS Digital Kft. a feltöltött dokumentumokat a feldolgozás időtartama alatt titkosítva több szerveren tárolja, ezzel mind az adatvesztés, mind az illetéktelen hozzáférés ellen magas szintű védelmet biztosít. A DocIT rendszer működésére, műszaki megfelelőségére vonatkozó további információkat a Szabályzat 2. számú melléklete tartalmazza.

A feldolgozást és hitelesítést követően a pdf fájlokat DWS Digital Kft. letölti a DocIT rendszerből, azok offline adathordozón kerülnek átadásra a Saint James Eye Clinic Kft. részére. DWS Digital Kft. ezt követően sem az iratokat, sem a pdf fájlokat nem tárolja, a teljes adatbázis törlésre kerül. Az átadást követően a Saint James Eye Clinic Kft. az elektronikus, hiteles iratokat saját szerverén tárolja, gondoskodik azok biztonságos hosszú távú megőrzéséről a jogszabályi előírások szerinti őrzési időtartamig.

6.2 A szabályzat hatálya, hitelesítendő iratok köre

Papíralapú dokumentumról hiteles elektronikus másolat készítése az alábbi irattípusok esetében történik:

a Saint James Eye Clinic Kft. a páciens aktáit digitalizáltatja és hitelesíti. Az akták az alábbi iratokat tartalmazzák: adatfelvételi lap, páciens nyilatkozat, orvosi lelet, zárójelentés, képalkotó eljárások felvételei, műtéti dokumentáció.

6.3 A másolatkészítés és validálás szabályai

1. A Saint James Eye Clinic Kft. 6.2. pontban meghatározott típusú iratait a Szolgáltatási szerződésben meghatározott módon adja át digitalizálásra a DWS Digital Kft. számára. Az átadott iratok teljeskörűségéért a Saint James Eye Clinic Kft. vállal felelősséget.
2. A másolatkészítés, a validálás és hitelesítés a DWS Digital Kft. telephelyén történik.
3. DWS Digital Kft. a papír alapú iratokat elektronikus másolattá alakítja át (a továbbiakban: digitalizálás vagy szkennelés).
4. A másolat készítésre jelen szabályzatban feljogosított személy - a több oldalas papíralapú iratok esetén - az iratokból kiszedi az összetűzést biztosító kapcsokat, majd vonalkódot helyez el az irat első oldalán. A vonalkód biztosítja az iratok közötti szeparációt, azaz, hogy egy fájlba egy irathoz tartozó képek/oldalak kerüljenek mentésre multipage pdf formátumba. A síkágyas szkenneren szkennelendő iratok esetén a vonalkódozás nem kötelező, ebben az esetben a szkenner vezérlő szoftverben kell meghatározni az összetartozó lapokat.
5. DWS Digital Kft. a digitalizálandó iratokat aktánként helyezi el a másolatkészítő eszközben, a szkennelés laponként történik. Az irat minden oldala – az üres oldalak automatikus kiszűrésével – szkennelésre kerül, függetlenül a lapok mértétől. A feldolgozás során az egy irathoz tartozó lapok szkennelése iratonként az aktában található eredeti oldal sorrendben történik.
6. Másolatkészítő a szkennelő eszköz segítségével legalább 300 dpi, maximum 400 dpi felbontású, színes pdf formátumú állományt készít.
7. A másolatkészítő a digitális képet a másolatkészítő eszközzel (szkenner) összekapcsolt szkenner vezérlő szoftveren keresztül ellenőrzi (validálás). Ennek során az alkalmazás automatikusan vizsgálja a képminőséget, az esetleges gyűrődéseket, elforgatást, összeolvasásokat, a másolatkészítő manuálisan ellenőrzi a futó sorszám szerinti darabszámot és a lapszámot. Rossz képminőség, gyűrődés, összeolvasás esetén a másolatkészítést korrigálni kell. Újraszkennelés esetén a hibás fájl törlésre kerül.
8. A másolat-készítő szoftver a képi fájlokon OCR (Optical Character Recognition) technológia segítségével teljes szöveg tartalom feldolgozást végez, melynek eredményeként a pdf fájlok szöveg tartalma kereshető lesz. A szövegesen kereshető pdf fájlok képi formátuma nem tér el az irat fizikai formátumától.
9. Kizárólag olyan elektronikus másolat készíthető, amely a papír alapú irat teljes tartalmát tartalmazza. Részleges másolat vagy kivonat nem készíthető.
10. A másolatkészítő szoftverből a létrejött képek exportálásra kerülnek, létrejönnek a pdf fájlok, melyek megfelelnek a ISO 32000-1:2008 (Portable Document Format – PDF) szabványnak.
11. Az exportálás során a másolatkészítő szoftver a validált másolatokat a szemklinika.docit.hu URL-en elérhető adatbázishoz kapcsolt SFTP szerveren helyezi el. Az exportálás előtt a mentés elérési útját a másolatkészítő szoftverben kell beállítani.
12. Exportálás előtt a DocIT szoftverben be kell állítani:
    - Az adott feltöltési csomagban található iratok típusát, DocIT rendszeren belüli elérési útját (mappáját), mely a rendszerben a hozzáférési jogosultságot meghatározza a regisztrált felhasználó számára.
    - másolatkészítés helyét
    - másolatkészítő szervezet nevét
    - másolatkészítési szabályzat elérési útját (URL)

13. A DocIT alkalmazás az FTP szerverről automatikusan olvassa be a digitális dokumentumokat, és betölti az adatbázisba.
14. A DocIT rendszerbe így feltöltött elektronikus fájlok „hitelesítésre váró” státuszba kerülnek. A rendszerben további ellenőrzési, validálási tevékenység végezhető. Majd a validálást követően a hitelesítés a „hitelesítésre váró” dokumentum csomagok esetén tömegesen indítható.

6.4 Hiteles másolatkészítés, hitelesítési eljárás

1. A DocIT rendszerbe beolvasott elektronikus másolat hitelesítésére a DWS Digital Kft. jogosult. A hitelesítés a DocIT rendszerben, a hitelesítési menüpont műszaki leírásában részletezett módon valósul meg.
2. Kizárólag olyan elektronikus másolat készíthető, amely a papíralapú dokumentum teljes tartalmát tartalmazza, részleges másolat vagy elektronikus kivonat nem készíthető.
3. A hiteles másolatkészítés folyamatában a másolatkészítés és a hitelesítés időben és térben elválik egymástól. Az eljárás zártságát ezekben az esetekben a kiépített szoftverkörnyezet műszaki leírásban bemutatott megoldása biztosítja.
4. A zárt rendszerben történő másolatkészítés alapján
5. A másolatkészítés sikeres, ha az eredeti papíralapú dokumentum és az elektronikus másolat képi és tartalmi megfelelése megállapítható, azaz az eredeti papíralapú dokumentum tartalmi és formai elemeinek megismerhetősége biztosított.
6. Ha a képi és tartalmi megfelelés nem állapítható meg, a másolatkészítést meg kell ismételni, valamint a képi és tartalmi megfelelés megállapítására nem alkalmas dokumentumot törölni kell.
7. A hitelesítés a DocIT rendszerben történik. A DocIT rendszer a hitelesítési művelet befejezésével egyidejűleg az elektronikus másolatot hitelesítési záradékkal látja el, és az elektronikus másolathoz az alábbi metaadatokat rendeli:

    a) Papíralapú dokumentum megnevezése;
    b) Papíralapú dokumentum fizikai méretei;
    c) Másolatkészítő szervezet elnevezése;
    d) Másolat képi vagy tartalmi egyezéséért felelős személy neve;
    e) Másolat hitelesítéséért felelős személy;
    f) Másolatkészítő rendszer megnevezése;
    g) Másolatkészítési szabályzat megnevezése és verziószáma;
    h) Másolatkészítés időpontja;
    i) Hitelesítés időpontja;
    j) Irányadó másolatkészítési rend elérhetősége.
8. A hitelesítési záradékkal ellátott elektronikus másolaton a DocIT rendszer elhelyezi a hitelesítést végző szervezet nevét (DWS Digital Kft.) tartalmazó elektronikus bélyegzőt és az időbélyeg szolgáltatótól származó időbélyeget. Az elektronikus dokumentum megváltoztathatatlanságát az elektronikus bélyegző, valamint a DocIT rendszer biztosítja a 2. mellékletben foglalt műszaki feltételek szerint. DWS Digital Kft. minősített tanúsítványon alapuló fokozott biztonságú elektronikus PAdES LTV aláírást és időbélyeget helyez el az elektronikus dokumentumokon, amely 10 éves érvényességi időt biztosít.

9. A hitelesítési záradék tartalmazza, hogy “Eredetivel megegyező hiteles másolat”, valamint az “Automatikus másolatkészítés” tényét.

6.5 Az eredeti papír alapú iratok további sorsa

A fenti lépésekkel a Saint James Eye Clinic Kft. már az átalakított elektronikus példány birtokába jutott, de a forrásul szolgáló papíralapú eredetik sorsát is rendezni szükséges.

A digitalizált, illetve feldolgozott iratok teljességének ellenőrzése szükséges. Az ellenőrzést a DWS Digital Kft. és a Saint James Eye Clinic Kft. együttesen végzi az iratokat létrehozó rendszer adatok alapján.

Eltérés esetén a konverziós folyamat teljes és tételes felülvizsgálata kezdődik, amely az eltérés okának feltárásáig, annak elhárításáig tart. Munkahibának minősül: minden, a manuális technológiában előírt folyamat elemtől való eltérés munkahibának minősül, ha az az ellenőrzés során eltérést eredményez. Ilyen például az adatok átírása, téves adatok helyesbítése.

A papír alapú és digitalizált iratokat a másolatkészítés és hitelesítés ellenőrzésének befejezéséig DWS Digital Kft. telephelyén őrzik. Amennyiben az ellenőrzés sikeresen, hiba nélkül lezárult, a hiteles digitális konverzió alá vont iratok irattári elhelyezéséről gondoskodni kell.

Az összegyűjtött iratokat DWS Digital Kft. a feldolgozás befejezésével a Szolgáltatási szerződés rendelkezései szerint elszállítja irattárolásra.

6.6 Másolatok hitelességének ellenőrzése

A pdf fájlok a hitelességre vonatkozó adatokat beágyazva tartalmazzák. Az elektronikus másolatok hitelessége az illetékesek számára egyszerűen ellenőrizhető az Adobe Reader program segítségével. A hitelesség ellenőrzése a DocIT programban archivált elektronikus iratok esetén a szoftver felületén is megtehető.

6.7 Elektronikus másolatok archiválása

A DWS Digital Kft. a feldolgozás időtartama alatt a DocIT rendszerben tárolja a hiteles elektronikus másolatokat. A feldolgozás befejezésével az elektronikus iratok offline adathordozón kerülnek átadásra a Saint James Eye Clinic Kft. részére.

Az hiteles elektronikus iratok további biztonságos archiválásáról, biztonsági mentések biztosításáról, az iratokhoz való hozzáférés szabályozásáról és a szabályok betartásáról a Saint James Eye Clinic Kft. gondoskodik.

Az orvosi iratok megőrzési kötelezettsége jelen jogszabályi előírások szerint 30 év. Ez idő alatt az elektronikus iratok felülhitelesítéséről, a hitelesség megőrzéséről a Saint James Eye Clinic Kft. gondoskodik.

Az elektronikus másolatok megőrzési kötelezettsége - az irat típusa szerint - a jogszabályi előírásoknak megfelelő ideig történik. Ezt követően az elektronikus iratok törléséről gondoskodni kell.

7 EGYÉB RENDELKEZÉSEK

A Szabályzat a közzététel napján lép hatályba.
A Szabályzatot a Saint James Eye Clinic Kft. webhelyén – bárki számára elérhető módon – közzé teszi, illetve amennyiben abban változás következik be, módosításáról és cseréjéről gondoskodik. Az előző állapotot a honlapon 10 évig kell megőrizni.

8 JOGSZABÁLYI MEGFELELŐSÉG

Jelen Szabályzat, a hiteles másolatkészítési folyamat kidolgozása és a Docit rendszer kialakítása az alábbi jogszabályok figyelembevételével történt:

- a digitális állampolgárság egyes szabályairól szóló 321/2024 (XI.6.) Kormány rendelet
- 910/2014/EU európai parlamenti és tanácsi rendelet („eIDAS rendelet”)
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

MELLÉKLETEK:

1. számú melléklet: Hiteles elektronikus másolat készítésére és validálására feljogosított személyek
2. számú melléklet: Műszaki dokumentáció

1. számú melléklet*:* Hiteles elektronikus másolat készítésére és validálására és hitelesítésre feljogosított személyek

Személy neve	Jogosultság	Munkavégzés helye (szervezet/cím)	Munkaköre	Érvényesség kezdete	Érvényesség vége
Szabó-Nagyné Monek Zsuzsanna	másolatkészítés, validálás, hitelesítés	DWS Digital Kft. 1116 Budapest, Sztregova utca 1	ügyvezető	2025.12.01	visszavonásig
Horváth-Gehér Szilvia	másolatkészítés, validálás, hitelesítés	DWS Digital Kft. 1116 Budapest, Sztregova utca 1	irat feldolgozó	2025.12.01	visszavonásig

2. számú melléklet: MŰSZAKI DOKUMENTÁCIÓ

1. Szkennelés:

A digitalizálás alá vont iratok aktánként egy irat egységenként kerülnek szkennelésre. A másolatkészítő felügyeli, hogy több irat nem kerül egy pdf fájlba.

2. Feltöltés DocIT rendszerbe

DWS által történő másolatkészítés esetén a szkennelt fájlok a szkennelő alkalmazásból közvetlenül kerülnek mentésre SFTP szerverre, ahonnan a fájlok DocIT rendszerbe beöltése azonnal megvalósul. A fájlok feltöltését követően a fájlok státusza „hitelesítésre váró” lesz.

3. Validálás

Következő fázisban történik a validálás. A DocIT rendszerbe feltöltést követően a másolatkészítő, validáló a DocIT rendszerben ellenőrzi a rögzített kép olvashatóságát, minőségét.
Amennyiben a kép minősége nem megfelelő (kép élesség, elmosódott, valamely képi információ vonatkozásában kétség merül fel), az iratot újra be kell szkennelni és a korábbi képet törölni kell. A törlés tényét, idejét, a fájl nevét, a műveletet végrehajtó felhasználót a DocIT rendszer automatikusan naplózza. Szkennelési javítás esetén, új fájl feltöltése történik.

4. Hitelesítés

Az elektronikus aláírás, a metaadat rendszer elektronikus példányra történő bekerülésének biztonságát a DWS DocIT rendszerének szerver oldali feldolgozása biztosítja. A másolat hitelesítését a DocIT rendszer végzi. A hitelesítés a validálást követően kerül elindítása DWS által a DocIT rendszerben. A rendszer automatikusan elhelyezi a dokumentumon a hitelesítés alkotóelemeit a „hitelesítésre váró” státuszú iratokon, melyek az alábbiak:

1. hitelesítési záradék szövege;
2. elektronikus dokumentum metaadatai;
3. elektronikus bélyegző;
4. időbélyeg.
5. A hitelesítési záradék szövege - „Az eredeti papíralapú dokumentummal egyező”, valamint “Automatikus másolatkészítés” – elhelyezésre kerül az elektronikus dokumentum képén.

Az elektronikus bélyegző használatához szükséges tanúsítványt a Microsec elektronikus tanúsítvány szolgáltató állítja ki. Az elektronikus bélyegző biztosítja az adott dokumentum lenyomatának segítségével a dokumentum sértetlenségét és az elektronikus bélyegző tulajdonosának letagadhatatlanságát.

Az időbélyeg azt igazolja, hogy az adott dokumentum egy adott időpillanatban már létezett. Az időbélyeget a Microsec időbélyegzés szolgáltató állítja ki. Az időbélyeg egy olyan adat, amely tartalmazza az időbélyegzett dokumentum lenyomatát, és az időbélyegzés időpontját, és az időbélyeget egy időbélyegzés szolgáltató hitelesíti saját aláírásával.

5. Elektronikus biztonság

5.1. DocIT rendszer alapadatok

A DocIT egy több-bérlős (multi-tenant) elektronikus dokumentumkezelő és irattári rendszer, amelyet a DWS Digital Kft. fejlesztett. Jelen dokumentum a DocIT rendszerre vonatkozó biztonsági tervet tartalmazza a NIS2 előírásainak megfelelően. A rendszer éles üzemben működik, több partnernél is használatban van felhőszolgáltatásként.

A rendszer azonosító adatai és működési környezete:

Szervezet neve: DWS Digital Kft.

Rendszer neve: DocIT

Engedélyezésért felelős vezető: Monek Zsuzsa (ügyvezető)

Rendszertulajdonos (IT vezető): Kiss Dániel

Rendszer állapota: Éles üzemben működik, több partnernél (multi-tenant)

Felhasználók köre: 1 rendszergazda (Kiss Dániel) és 8–10 végfelhasználó; technikai felhasználó nincs

Kapcsolódó rendszer: NAV Online Számla (külső számlaadat-szolgáltató rendszer)

Üzemeltetési környezet: A rendszer a Rackforest Zrt. felhő infrastruktúráján fut; a szervereket és hálózatot a Rackforest biztosítja, míg a szoftver fejlesztését és ügyféltámogatását a DWS végzi

Biztonsági osztály: Alap (a rendszer bizalmassági, sértetlenségi és rendelkezésre állási követelményei alap besorolás alá esnek)

5.2. Adattárolás és titkosítás

A DocIT alkalmazás kliens-oldali elérése kizárólag biztonságos HTTPS kapcsolaton (TLS) keresztül történik, így az adatátvitel titkosított. A dokumentumokat a rendszer a kiszolgáló szerver fájlrendszerén AES-256-CBC algoritmussal titkosítva tárolja, így illetéktelen hozzáférés esetén sem olvashatók a fájlok tartalmai. Az alkalmazás- és adatbázis-szerver tűzfalakkal védett, és csak a szükséges hálózati portok vannak megnyitva (pl. 443/tcp a HTTPS forgalom számára).

5.3. Biztonsági mentések

Az adatbázisokról és a feltöltött dokumentumokról napi szinten titkosított biztonsági mentés készül, melyet az adatfeldolgozó DWS végez. A mentések biztonságos, jogosulatlan hozzáféréstől védett tárolóhelyre kerülnek. Amennyiben egy dokumentum-feldolgozási folyamat lezárult és a keletkezett elektronikus dokumentumokat átadták az adatkezelő (ügyfél) részére, a DWS – mint adatfeldolgozó – törli az adott feldolgozáshoz tartozó teljes adatbázist és annak minden biztonsági mentését, ezzel is minimalizálva az adatok további fennmaradását és kitettségét. Rutin üzemeltetés során a mentésekből szükség esetén helyreállítás végezhető, biztosítva az adatok folytonosságát egy esetleges incidens (adatvesztés) után.

5.4. Külső integrációk

A DocIT rendszer összeköttetésben áll a Nemzeti Adó- és Vámhivatal (NAV) Online Számla rendszerével. A két rendszer közti adatkommunikáció szabványos, biztonságos REST API-n keresztül, HTTPS protokollal történik, megfelelő hitelesítéssel. Ennek köszönhetően a DocIT képes integrált módon kezelni a számlaadat-szolgáltatást, miközben az adatcsere titkosított csatornán zajlik. Nincs egyéb, nyilvános hálózatra kinyitott interfész a rendszeren, a külső kapcsolatokat minimálisra korlátoztuk (jellemzően csak a HTTPS kommunikáció a webes kliens és a NAV rendszer felé engedélyezett).

5.5. Hozzáférési intézkedések

A rendszerhez való hozzáférés szigorú azonosítási és jogosultságkezelési szabályok mentén történik a jogosulatlan belépések megakadályozása érdekében:

5.6. Felhasználói fiókok és hitelesítés

A DocIT rendszer használatához minden felhasználónak előzetesen regisztrált, névre szóló felhasználói fiókkal kell rendelkeznie; anonim hozzáférés nem lehetséges. A bejelentkezés felhasználónévvel és jelszóval történik. A jelszavakra erős követelmények vonatkoznak: minimum 8 karakter hosszúak, tartalmaznak kis- és nagybetűt, számot és speciális karaktert. A jelszavakat a rendszer egyirányú bcrypt algoritmussal hashelve tárolja, így azok visszafejtése rendkívül nehéz. További biztonsági lehetőségként a felhasználók kétfaktoros hitelesítést is beállíthatnak Google Authenticator alkalmazás használatával, ami a sikeres belépéshez egy egyszer használatos kód megadását követeli meg a jelszó mellett. Nincsenek megosztott vagy általános jelszavú fiókok; technikai (gépi) felhasználói fiókok sincsenek a rendszerben – minden hozzáférés konkrét személyhez kötött. Új felhasználói fiókot kizárólag a rendszergazda/adminisztrátor hozhat létre, ellenőrzött keretek között.

5.7. Jogosultsági rendszer

A DocIT többszintű jogosultságkezelő rendszerrel rendelkezik. A hozzáférés szerepkörökhöz (jogosultsági csoportokhoz) kötött: adminisztrátori jogosultsággal tetszőleges számú szerepkör definiálható, és ezekhez finoman szabályozott jogosultságok rendelhetők. A jogosultságok az irattípus–mappa mátrix mentén kerülnek meghatározásra, és négy fő műveleti szintet különböztetnek meg: keresés/megtekintés, adatmódosítás, letöltés és törlés. Minden egyes szerepkörnél beállítható, hogy az adott dokumentumtípus adott mappájában mely műveletek engedélyezettek. Egy felhasználó több szerepkörrel is rendelkezhet; ilyenkor a hozzáférési jogai az összes hozzárendelt szerepkör egyesített jogosultsági halmaza alapján alakulnak ki. E rendszer biztosítja, hogy a felhasználók csak azokhoz az adatokhoz és funkciókhoz férjenek hozzá, amelyekhez a munkakörük folytán szükséges, ezzel minimalizálva a túlzott jogosultságokból eredő kockázatokat. Az adminisztrátori fiók teljes körű hozzáféréssel bír a rendszer összes funkciójához és adatához, míg az általános felhasználók csak a számukra engedélyezett modulokat/lapokat érik el.

5.8. Védelmi intézkedések

A DocIT rendszert több védelmi mechanizmus óvja a jogosulatlan hozzáféréstől, a rosszindulatú támadásoktól és a kártevőktől, valamint biztosítja az adatok integritását és a tevékenységek nyomon követhetőségét:

5.9. Hálózat- és peremvédelem

A kiszolgáló szerver(ek) hálózatbiztonságát tűzfal (UFW) biztosítja, amely alapértelmezetten tilt minden forgalmat, és csak a minimálisan szükséges portokat engedélyezi (pl. 443/tcp a HTTPS szolgáltatáshoz, illetve korlátozottan 22/tcp a rendszergazdai adminisztrációhoz). A nyilvános szolgáltatások elé Cloudflare webalkalmazás tűzfalat (WAF) integráltunk, amely szűri a forgalmat és védelmet nyújt a DDoS és egyéb webes támadások ellen. Emellett a szerveren fail2ban figyeli a bejelentkezési kísérleteket és más gyanús tevékenységeket: ismétlődő hibás próbálkozások esetén az érintett kliens IP-címét automatikusan kitiltja egy időre, megelőzve a brute force támadásokat. Ezek az intézkedések együttesen erős peremvédelmetbiztosítanak, megakadályozva, hogy illetéktelen vagy rosszindulatú hálózati forgalom elérje a rendszert.

5.10. Alkalmazásbiztonság

A DocIT szoftver fejlesztése során kiemelt figyelmet kapott a biztonságtudatos tervezés és kódolás. A Laravel 9 keretrendszer beépített védelmi mechanizmusait kihasználva az alkalmazás ellenáll a tipikus webes támadásoknak. Implementálva van az SQL injection elleni védelem, így a bemenő adatok megfelelően kezeltek és nincsenek közvetlenül beillesztve az SQL utasításokba. Cross-Site Scripting (XSS) elleni védelem gondoskodik róla, hogy a felhasználói tartalmak ne okozhassanak kliens oldali káros kódvégrehajtást. Cross-Site Request Forgery (CSRF) tokenek védik az űrlapokat a jogosulatlan parancs-végrehajtástól. A bejelentkezési funkció rate limiting mechanizmussal van ellátva, ami korlátozza a rövid időn belül megengedett belépési próbálkozások számát, megelőzve a jelszó-kitalálási támadásokat. Az alkalmazás logikájában érvényesül a Laravel Gate alapú hozzáférés-vezérlés: bizonyos műveletek végrehajtása csak meghatározott jogosultsági szint mellett lehetséges, így a rendszer a programkódban is ellenőrzi, hogy egy művelethez a felhasználó rendelkezik-e megfelelő jogosultsággal. Továbbá a rendszerarchitektúra úgy lett kialakítva, hogy szolgáltatás megtagadásos támadások (DDoS) ellen is védett legyen (pl. a fent említett Cloudflare réteg révén és megfelelő erőforrás-kapacitással).

5.11. Vírusvédelem

A DocIT rendszerben szigorúan szabályozott, hogy a felhasználók milyen fájltípusokat tölthetnek fel. Csak biztonságos, elvárt típusú dokumentumok engedélyezettek, futtatható állományok feltöltése tiltott. A feltöltött fájlok nem egy weben közvetlenül elérhető vagy futtatásra alkalmas könyvtárba kerülnek, hanem elkülönítve, titkosított formában tárolódnak, így még egy esetleges rosszindulatú fájl sem tud közvetlenül károkat okozni a kiszolgálón. Emellett a szervereken vírusirtó szoftver fut, amely az összes feltöltött elektronikus dokumentumot ellenőrzi ismert kártevők ellen. Ez biztosítja, hogy a dokumentumtárba ne kerülhessen fertőzött fájl, illetve egy feltöltött esetleges vírust a rendszer ne továbbítson a felhasználók felé. On-premise telepítés esetén a DWS vállalja a vírusvédelem beállítását és karbantartását a felhasználó által biztosított szerveren is, ugyanolyan szintű védelmet garantálva, mint a felhőben.

5.12. Biztonsági frissítések

A DocIT alkalmazást és a mögöttes szerver operációs rendszert folyamatosan karbantartjuk a legújabb biztonsági frissítések alkalmazásával. Az éles üzemi környezetben a szoftverek és komponensek biztonsági frissítéseit legalább havi rendszerességgel telepítjük, illetve szükség esetén azonnal, ha kritikus sérülékenységre kiadásra kerül javítás. Ez biztosítja, hogy a rendszer mindig naprakész legyen, és a már ismert biztonsági rések ne legyenek kihasználhatók. A frissítések telepítése kontrollált folyamat keretében zajlik, tesztelést követően, hogy ne okozzon üzemi kiesést. On-premise üzemeltetésnél ugyanezen elvek alapján a DWS végzi el a frissítéseket a ügyfél szerverén, garantálva a konzisztens védelmi szintet.

5.13. Naplózás és auditálás

A rendszer minden fontos eseményt és műveletet naplóz annak érdekében, hogy utólag rekonstruálhatók legyenek az adatkezelési és hozzáférési események. Naplózásra kerül többek között az összes rekord törlése, a dokumentumokhoz tartozó bármilyen metaadat módosítása, továbbá a dokumentumok megtekintése és letöltése is. A törölt rekordok nem semmisülnek meg azonnal: inaktivált státusszal egy elkülönített archív naplóállományba kerülnek, ahol 1 évig megőrződnek. Ez idő alatt – megfelelő jogosultsággal (rendszeradminisztrátor) – szükség esetén az archivált adatok visszaállíthatók, azaz egy tévesen törölt dokumentum helyreállítható. A naplóadatok kezeléséről (tárolás, archiválás, selejtezés) és biztonságos őrzéséről a DWS gondoskodik. A rendszer adminisztrátorai számára a felhasználói felületen elérhető egy naplómegtekintő modul, ahol szűrők segítségével lekérdezhetők a történések (pl. egy adott felhasználó tevékenységei vagy egy adott dokumentum előzményei), és a naplóadatok exportálhatók további elemzés vagy

riportkészítés céljából. Dokumentumszinten is nyomon követhetők az események: egy adott irat adatlapján a felhasználók láthatják a dokumentummal kapcsolatos összes releváns művelet listáját, beleértve az adatmódosításokat mezőszintű részletezettséggel. Ezek az auditálási lehetőségek elősegítik a szabályszerű működés ellenőrzését és egy esetleges incidens kivizsgálását.

5.14. Adatok integritása és hitelessége:

A DocIT rendszer biztosítja, hogy az általa kezelt elektronikus dokumentumok hitelessége és változatlansága igazolható legyen. Különösen, a papíralapú dokumentumokból előállított hiteles elektronikus másolatok (PDF fájlok) a feltöltés/feldolgozás során elektronikus bélyegzővel és időbélyeggel vannak ellátva. Az elektronikus bélyegző (digitális aláírás) garantálja a dokumentum megváltoztathatatlanságát: a tartalom utólagos módosítása észlelhető, és a bélyegző tulajdonosa (DWS vagy az adott partner) nem tagadhatja le a dokumentum eredetiségét. Az időbélyeg pedig rögzíti a hitelesítés pontos idejét. E cryptográfiai védelem biztosítja, hogy a DocIT-ben tárolt fontos dokumentumok jogilag is megfeleljenek a hitelesség és sértetlenség követelményeinek, kizárva a dokumentumok észrevétlen manipulációját. Ezen intézkedések révén a rendszer által kezelt iratok megbízhatósága és bizonyító ereje garantált.