**Az Eatrend Kft.**

**MÁSOLATKÉSZÍTÉSI SZABÁLYZATA**

**Verzió: 1.0**

**2025. július 1.**

**………..........………………**

Takács Zsolt

ügyvezető

**Verziókövetés:**

|  |  |  |
| --- | --- | --- |
| **Verzió** | **Módosítás tartalma** | **Hatálybalépés** |
| 1.0 | Másolatkészítési szabályzat 1.0 | 2025.07.01 |
|  |  |  |
|  |  |  |
|  |  |  |

TARTALOM

[**1 A SZABÁLYZAT CÉLJA 3**](#_re2a9oiwflf5)

[**2 FOGALMAK 3**](#_ei75c520uxw)

[**3 A MÁSOLAT KÉSZÍTÉS FOLYAMATA 4**](#_ksi007p741kr)

[3.1 DocIT elektronikus irattári rendszer 4](#_yg8u0sohiuyp)

[3.2 A szabályzat hatálya, hitelesítendő iratok köre 5](#_41a0mblniktl)

[3.3 Az automatikus másolatkészítés és a validálás szabályai 5](#_kfg3l446pq7)

[3.4 Hiteles másolatkészítés, hitelesítési eljárás 7](#_po314qbb5a80)

[**4 EGYÉB RENDELKEZÉSEK 9**](#_fcrgt42jzx25)

[**5 (1).számú melléklet - Hiteles elektronikus másolat készítésére és validálására feljogosított személyek 10**](#_ww8eltdgnvts)

[**6 (2). számú melléklet - MŰSZAKI DOKUMENTÁCIÓ 11**](#_5bt8zbsqejui)

[6.1 Műszaki megfelelés 11](#_tvmbrcezl5pt)

[6.2 Rendszer biztonság 12](#_rjd7siy7tbm2)

# A SZABÁLYZAT CÉLJA

Az Eatrend Kft. Másolatkészítési Szabályzatának (a továbbiakban: Szabályzat) célja az Eatrend Kft. **papíralapú dokumentumainak hiteles elektronikus irattá történő átalakítására** vonatkozó alapvető és egységes szabályok meghatározása a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény, az 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 Szabályzat a vonatkozó jogszabályokkal összhangban tartalmazza az Eatrend Kft-hez érkező és ott keletkező papír alapú számlák, könyvelési bizonylatok, gazdasági iratok, jognyilatkozatot nem tartalmazó munkaügyi iratok hiteles elektronikus másolattá alakításának eljárási rendjét, valamint a hiteles elektronikus számlák hiteles archiválásának megvalósítását és műszaki feltételeit.

Az Eatrend Kft. könyvelési iratainak és dolgozói jognyilatkozatot nem tartalmazó munkaügyi iratainak szkennelésével, feldolgozásával és hitelesítésével jelen Szabályzat rendelkezéseinek megfelelően a DWS Digital Kft-t (a továbbiakban: DWS) bízza meg.

# 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.

**Elektronikus másolat**: Valamely papíralapú dokumentumról e szabályzat előírásai alapján készült, azzal képileg vagy tartalmilag egyező, joghatás kiváltására alkalmas elektronikus eszköz útján értelmezhető adategyüttes.

**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 a megismerhetőségét, de nem biztosítja a képi megfelelést.

**Másolatkészítő rendszer:** A másolatkészítés során alkalmazott hardver, szoftver, valamint ezek együttese.

**Másolatkészítés dátuma:** Az elektronikus másolat készítése során a képi és/vagy tartalmi egyezőség ellenőrzésének dátuma.

**Digitalizálás**: Olyan eljárás, amely az analóg felépítésű információt számítástechnikai eszközök számára feldolgozható, digitális információvá alakítja át.

**Metaadat:** A tárolt dokumentumot leíró ismertető adatok.

**Automatikus másolatkészítés**: másolatkészítés külső beavatkozástól mentes zárt rendszerben történik.

**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.

# A MÁSOLAT KÉSZÍTÉS FOLYAMATA

## DocIT elektronikus irattári rendszer

DWS végzi az Eatrend Kft. iratainak nagytömegű szkennelését és a digitalizált fájlok feltöltését az elektronikus irattárba, valamint a visszakeresést biztosító adatok rögzítését, továbbá a jelen szabályzat részét képező validálást és hitelesítést. DWS a feltöltött dokumentumokat titkosítva több szerveren tárolja, ezzel mind az adatvesztés, mind az illetéktelen hozzáférés ellen magas szintű védelmet biztosít.

Eatrend Kft. elektronikus dokumentumainak feldolgozására a DWS által biztosított felhő alapú DocIT rendszert használja. DWS az iratok feldolgozásának időtartama alatt biztosítja az Eatrend Kft. részére az elektronikus irattár szolgáltatást: a http://eatrend.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.

A DocIT rendszer végzi:

* az elkészült képi fájlok zárt rendszerben tárolását
* az automatikus másolatkészítés során létrejött fájlok megjelenítését, és validálási lehetőségét a képek szerkesztése nélkül.
* hiteles digitális konverziót.
* A fájlokhoz rendelt visszakeresést biztosító adatok ellenőrzését.

DWS a feltöltött dokumentumokat titkosítva több szerveren tárolja, ezzel mind az adatvesztés, mind az illetéktelen hozzáférés ellen magas szintű védelmet biztosít.

A hitelesítést követően a fájlok a kapcsolódó adat állománnyal együtt exportálásra kerülnek, és offline adathordozón kerülnek átadásra Eatrend Kft. részére. Ezt követően a hitelesített fájlok törlésre kerülnek a DocIT rendszerben, azok archiválásáról saját szerverén Eatrend Kft. gondoskodik.

## A szabályzat hatálya, hitelesítendő iratok köre

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

**Gazdasági iratok**:

* Költség számlák és mellékletei
* Bevétel számlák
* Pénztárbizonylatok
* Bankbizonylatok

**Munkaügyi iratok:**

* Munkavállalók személyi aktáinak meghatározott iratai:
* Munkavállalói adóbevallások
* Havi bérszámfejtés iratai
* Munkaidő igazolás iratai
* Egyéb munkaügyi adatszolgáltatás és elszámolás iratai

## Az automatikus másolatkészítés és a validálás szabályai

* + 1. Eatrend a 3.2. pontban meghatározott típusú iratait a DWS Digital Kft-vel kötött Vállalkozási szerződésben meghatározott módon adja át digitalizálásra a DWS számára. Az átadott iratok teljeskörűségéért az Eatrend vállal felelősséget. Az átadás-átvételt dosszié jegyzék kíséri, melyen feltüntetésre kerül a szervezet megnevezése, a szervezeti egység, az irattípus és a keletkezés időintervalluma.
    2. A másolatkészítés és hitelesítés a DWS telephelyén történik.
    3. DWS a papír alapú, 3.2. pontban megjelölt típusú dokumentumokat hiteles elektronikus másolattá alakítja át (a továbbiakban: digitalizálás).
    4. A másolatkészítésre jelen szabályzatban feljogosított személy a több oldalas papíralapú iratok esetén vonalkódot helyez el az irat első oldalán, majd a digitalizálandó küldeményeket kötegelve helyezi el a másolatkészítő eszközben. A vonalkód biztosítja a dossziék azonosítását. Egy dosszié tartalma 50, de max. 100 oldalanként kerül multipage pdf fájlba mentésre.
    5. DWS a nagyteljesítményű szkenner segítségével legalább 300 dpi felbontású, pdf formátumú állományt készít.
    6. A másolatkészítő a digitális képet a másolatkészítő eszközzel összekapcsolt KOFAX alkalmazáson keresztül ellenőrzi (validálás). Ennek során az alkalmazás automatikusan vizsgálja a képminőséget, az esetleges gyűrődéseket, összeolvasásokat, ellenőrzi a futó sorszám szerinti darabszámot és a lapszámot. Rossz képminőség, gyűrődés, összeolvasás esetén a másolatkészítést meg kell ismételni, a hibás fájl törlésre kerül.
    7. A másolatkészítő rendszer a validált másolatokat SFTP szerveren helyezi el. A DocIT alkalmazás a szerverről automatikusan olvassa be a digitális dokumentumokat, betölti saját adatbázisába.
    8. A digitalizálás eredményeként a papír alapú iratok minden oldala egy multipage pdf formátumú fájlba kerül. A dokumentumról csak olyan másolat készül, mely a papír alapú dokumentum teljes tartalmát tartalmazza, tehát nem készül sem részleges másolat, sem elektronikus kivonat. Az iraton szkennelés előtt kizárólag iratkezelési rájegyzések tehetők (érkeztetési, iktatási bélyegzők kitöltése, iktatószám), figyelemmel arra, hogy azok az irat tartalmát ne takarják ki.

Minden, a másolat készítésben részt vevő személy a vonatkozó jogszabályi előírások (Polgári Törvénykönyv, Munka Törvénykönyve) alapján a tevékenységéért felelősséggel tartozik. A hiteles másolatkészítés során az elkülönült szerepkörök biztosítják a felelősség megosztását.

Jelen szabályzat szerinti hiteles másolatot csak a DWS erre a feladatra kijelölt munkatársa (a továbbiakban: másolatkészítő) készíthet. A másolat készítésére kijelölt, szkennelési és validálási tevékenységet ellátó munkatársak nevét a szabályzat 1. számú melléklete tartalmazza.

* + 1. **Az ellenőrzés** során a másolatkészítő felelős minden szkennelt irat esetén tételesen ellenőrzi, megvizsgálja, hogy:
* az irat maradéktalanul és teljeskörűen szkennelésre került,
* a képi fájl minősége megfelelő, a másolatkészítés során nem történt másolási hiba (gyűrődés, elcsúszás, kamerahiba stb.)
* az irat olvashatóságát, képminőségét.
  + 1. **Hibajavítás**: abban az esetben, ha a képi fájlok minősége nem megfelelő, a képek hiányosak, sérültek, a felelős a hibás fájlt törli, és gondoskodik az irat újbóli szkenneléséről.
    2. **Másolatkészítő azonosítása**: A másolatkészítő és ellenőrzést végző személy DocIT rendszer felhasználó, saját azonosítójával és jelszavával, kétfaktoros azonosítással lép be a rendszerbe, a DocIT rendszer ez alapján azonosítja a másolatkészítő és validáló személyt.

## Hiteles másolatkészítés, hitelesítési eljárás

* + 1. A DocIT rendszerbe beolvasott elektronikus másolat hitelesítésére a DWS jogosult. A hitelesítés a DocIT rendszerben, a hitelesítési menüpont műszaki leírásban részletezett módon valósul meg, az ellenőrzést követően a “Hitelesítés indítása” funkció indításával.
    2. 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.
    3. 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.
    4. 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. A törölt képfájlok ténylegesen nem kerülnek törlésre az adatbázisból, azok törölt státuszba kerülnek, mely státusz szükség szerint visszaállítható.
    5. 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.

* + 1. A hitelesítési záradékkal ellátott elektronikus másolaton a DocIT rendszer elhelyezi a hitelesítést végző szervezet nevét tartalmazó elektronikus bélyegzőt és az időbélyeg szolgáltatótól származó időbélyeget. A hiteles digitális konverzió 10 évig érvényes PAdES LTV szintű aláírással és 2 időbélyeggel történik. Az elektronikus dokumentum megváltoztathatatlanságát az elekidőbélyegettronikus bélyegző, valamint a DocIT rendszer biztosítja a 2. mellékletben foglalt műszaki feltételek szerint.
    2. A hitelesítési záradék tartalmazza, hogy “Eredetivel megegyező hiteles másolat”, valamint az “Automatikus másolatkészítés” tényét.
  1. **Az eredeti papír alapú iratok további sorsa**
     1. A fenti lépésekkel az Eatrend Kft. már az átalakított elektronikus példány birtokába jutott, de a forrásul szolgáló papíralapú eredetik sorsát is rendezni szükséges.
     2. A digitalizált, illetve feldolgozott iratok teljességellenőrzése szükséges. Az ellenőrzést az Eatrend Kft. is elvégzi a rendszeradatok alapján a 3.4. pontban leírtak szerint.
     3. Eltérés esetén a konverziós folyamat teljes és tételes felülvizsgálata kezdődik, amely az eltérés okának feltárásáig, annak elhárításáig tart.
     4. 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.
     5. A papír alapú és digitalizált iratokat a másolatkészítés és hitelesítés ellenőrzésének befejezéséig a DWS Digital Kft. telephelyén őrzik. Amennyiben az ellenőrzés sikeresen, hiba nélkül lezárult, a hiteles digitális konverzió alá vont iratok megsemmisíthetők. Az összegyűjtött iratok megsemmisítéséről a DWS Digital Kft. gondoskodik.
     6. **Hibajavítás**: a képi fájlok minőségével és teljességével kapcsolatban nem merülhet fel kifogás.
  2. **Másolatok hitelességének ellenőrzése**

A hitelesség a DocIT rendszerben ellenőrizhető a dokumentum elektronikus adatlapján.

A hiteles másolatok a rendszerből letöltés esetén is megőrzik hitelességüket. Az így letöltött elektronikus másolatok hitelessége egyszerűen ellenőrizhető az ingyenesen letölthető Adobe Reader program segítségével. A PDF állományok az ellenőrzéshez szükséges összes információt beágyazva tartalmazzák. Mind az aláíráshoz, mind az időbélyeghez használt tanúsítvány visszavezethető az EU megbízható listákban (EU Trusted Lists) található főtanúsítványokig, amely főtanúsítványok letöltését az Adobe Reader 11-es vagy újabb verziói automatikusan elvégzik. A hitelesítési záradékot és metaadatokat az összes hiteles PDF állományba egyenként csatolt szöveges állomány tartalmazza.

A DocIT rendszerből letöltött hiteles másolat módosítása és manipulációja esetén annak hitelessége elvész.

# EGYÉB RENDELKEZÉSEK

A Szabályzat a közzététel napján lép hatályba.

A szabályzat alkalmazására az Eatrend Kft., valamint a másolatkészítés és hitelesítés vonatkozásában, az érvényben lévő vállalkozási szerződés alapján a DWS Digital Kft. valamennyi munkavállalója köteles.

A Szabályzatot az Eatrend Kft. webhelyén – bárki számára elérhető módon – közzé kell tenni, illetve amennyiben abban változás következik be, módosításáról és cseréjéről gondoskodni szükséges. Az előző állapotot a honlapon 10 évig kell megőrizni.

Budapest, 2025. június 1.

**…………………………………**

Takács Zsolt ügyvezető

# (1.) SZÁMÚ MELLÉKLET - Hiteles elektronikus másolat készítésére és validálására feljogosított személyek

***Szabó-Nagyné Monek Zsuzsanna,*** *DWS Digital Kft. - hitelesítés indítása*

***Horváth-Gehér Szilvia,*** *DWS Digital Kft. - szkennelés, validálás*

***Kovács Zsuzsanna****, DWS Digital Kft. - szkennelés, validálás*

# (2). SZÁMÚ MELLÉKLET - MŰSZAKI DOKUMENTÁCIÓ

## Műszaki megfelelés

* + 1. Szkennelés:

A digitalizálás alá vont iratok dosszié egységenként kerülnek szkennelésre. A másolatkészítő felügyeli, hogy egy dosszié tartalma 50-100 oldalas egységekben egy pdf fájlba kerüljön.

A másolatkészítés nagyteljesítményű lapadagolós szkennerrel és az azt vezérlő KOfax Express szoftverrel történik, melynek eredményeként létrejött képi fájl SFTP szerverre kerül exportálára.

* + 1. 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”.

* + 1. 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.

* + 1. Hitelesítés

Az elektronikus aláírás, a metaadatrendszer 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 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.

## Rendszer biztonság

* + 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)

* + 1. 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).

* + 1. 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.

* + 1. 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).

* + 1. Hozzáférési intézkedések

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

* + - 1. 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.

* + - 1. 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.

* + 1. 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:

* + - 1. 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 peremvédelmet biztosítanak, megakadályozva, hogy illetéktelen vagy rosszindulatú hálózati forgalom elérje a rendszert.

* + - 1. 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 szolgáltatásmegtagadásos támadások (DDoS) ellen is védett legyen (pl. a fent említett Cloudflare réteg révén és megfelelő erőforrás-kapacitással).

* + - 1. 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.

* + - 1. 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.

* + - 1. 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.

* + - 1. 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.