Biztonsági politika

Safety Software | Aktualizacja: 17.12.2025 | https://safetysoftware.eu

A Safety Software (SaaS) Alkalmazásbiztonsági Szabályzat

Azonosító: SE-2026-V2
Frissítés: 2026-03-05

1. Cél és hatály

Jelen Biztonsági Szabályzat meghatározza a Safety Software alkalmazás keretében, Software as a Service (SaaS) modellben nyújtott szolgáltatás során kezelt információk és adatok védelmének szabályait.

A dokumentum a Safety Software szolgáltatásban az alkalmazást használó felhasználók biztonságára vonatkozik, és a Szabályzat, valamint az Adatvédelmi Szabályzat kiegészítését képezi.

A Szabályzat tájékoztató jellegű, és leírja a Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polska (a továbbiakban: „Adminisztrátor”) által alkalmazott alapvető technikai és szervezési intézkedéseket.

2. Felelősségi modell

A rendszer megosztott felelősségi modellben működik:

1. **Az Adminisztrátor (Safety Software)** felel az alkalmazáskód biztonságáért, a bejelentkezési, jogosultságkezelési és munkamenet-mechanizmusokért, az adatok alkalmazási rétegben történő védelméért, a biztonsági mentések készítéséért, valamint a biztonsági incidensekre adott válaszokért.

2. **Az infrastruktúra- és kiegészítő szolgáltatók** felelnek az általuk nyújtott szolgáltatások körébe tartozó elemek biztonságáért.

3. **Az Ügyfél** felel saját eszközeinek, jelszavainak, a felhasználói identitásoknak a biztonságáért, valamint a csapatán belüli hozzáférések kezeléséért.

3. Az alkalmazás biztonsági elvei

1. Az adatátvitel kizárólag TLS titkosítás használatával történik.

2. A felhasználói munkamenetek **HttpOnly**, **Secure** (titkosított kapcsolatokhoz) és **SameSite** attribútumokkal rendelkező cookie-k használatával vannak védve. Hitelesítést követően a munkamenet-azonosító rotációja történik.

3. A munkamenetekre tétlenségi és maximális időtartam-korlátok vonatkoznak.

4. A rendszer állapotát megváltoztató kérések szerveroldalon ellenőrzött CSRF tokenekkel vannak védve.

5. Az alkalmazás szigorú tartalombiztonsági szabályzatot alkalmaz, beleértve a nem engedélyezett szkriptek futtatását korlátozó mechanizmusokat, valamint a böngészők szabványos biztonsági fejléceit.

6. Visszaéléseket korlátozó mechanizmusokat alkalmazunk, beleértve a rate limitinget és a brute force bejelentkezési kísérletek elleni védelmet.

7. Minden művelet felhasználói és szervezeti kontextusban kerül végrehajtásra; a jogosulatlan hozzáférés blokkolásra kerül.

4. Titkosítás és adatvédelem

1. A felhasználói jelszavak **bcrypt** algoritmussal kerülnek tárolásra.

2. Az adatbázisban tárolt kiválasztott érzékeny adatok a borítékos adattitkosítási modell alkalmazásával védettek. A kriptográfiai kulcsok kezelése külön, külső kulcskezelő rendszerben történik.

3. Indokolt esetben olyan mechanizmusokat alkalmazunk, amelyek a keresési vagy azonosítási funkciók fenntartása mellett korlátozzák az adatok kitettségét, anélkül, hogy a teljes értékeket nyílt formában kellene tárolni.

5. Biztonsági mentés és helyreállítás (BCP/DR)

1. Rétegezett megközelítést alkalmazunk a biztonsági mentésekhez: helyi mentések a gyors visszaállításhoz, valamint az elsődleges környezeten kívül tárolt mentések.

2. Az elsődleges környezeten kívül tárolt mentések inkrementálisan készített környezetképeket tartalmaznak. Ezek titkosítottak, rendszeresen validáltak, és helyreállítási tesztek tárgyát képezik.

3. Az adatbázis alkalmazási szinten konzisztens mentésekkel van védve. Ezen felül helyi adatbázis-dumpok is fenntartásra kerülnek a gyors visszaállítás támogatására.

4. A mentések integritása ellenőrző mechanizmusokkal, többek között ellenőrző összegekkel kerül verifikálásra.

5. A mentési folyamat automatizált, naponta fut, és a feladatok sikerességének, illetve sikertelenségének monitorozása alá esik.

6. Rendszeresen adat-helyreállítási tesztek kerülnek végrehajtásra, legalább kiválasztott fájlok visszaállítását magukban foglalva.

6. Monitorozás és riasztások

1. A rendszer rögzít bizonyos biztonsági eseményeket és adminisztratív műveleteket, különösen a hitelesítéssel, hozzáférési kísérletekkel és a kritikus folyamatok működésével összefüggésben.

2. Monitorozási mechanizmusokat és automatikus riasztásokat alkalmazunk feladatok sikertelensége, kritikus hibák és olyan események esetén, amelyek visszaélésre vagy biztonsági incidensre utalhatnak.

3. A naplókhoz és operatív információkhoz való hozzáférés jogosult személyekre korlátozott.

7. Infrastruktúra és a biztonság fenntartása

1. Az adminisztratív hozzáférés jogosult személyekre korlátozott, és erős hitelesítési mechanizmusokkal védett, beleértve a kulcsalapú hitelesítést.

2. A közvetlen bejelentkezés privilegizált fiókba ki van kapcsolva, vagy a minimális jogosultság elvével összhangban korlátozott.

3. Forgalomszűrési mechanizmusokat, brute force hozzáférési kísérletek elleni védelmet, valamint az infrastruktúra-események monitorozását alkalmazzuk.

4. A biztonsági frissítések rendszeresen kerülnek bevezetésre.

5. A rendszer kiszolgálásához használt levelezési szolgáltatások az átvitel titkosításával és visszaéléseket korlátozó mechanizmusokkal védettek.

8. Szolgáltatók és integrációk

1. Amennyiben a rendszer külső szolgáltatásokat vagy kiegészítő integrációkat vesz igénybe, a megoldások kiválasztása figyelembe veszi az adatbiztonságot, a minimalizálás elvét, valamint az átadott információk körének ellenőrzését.

2. A külső szolgáltatásokkal való kommunikáció titkosított adatátvitellel történik.

9. Incidensek bejelentése

Az alkalmazás biztonságával kapcsolatos bejelentéseket vagy incidensgyanúkat az alábbi címre kell küldeni:

office@safetysoftware.eu
Üzenet tárgya: SECURITY

A bejelentések elemzése a belső incidenskezelési eljárás szerint történik.

10. Megfelelőség és joghatóság

1. A biztonsági intézkedések tervezése és fenntartása a hatályos jogszabályok, beleértve a **GDPR** követelményeit, valamint az elismert információbiztonsági gyakorlatok figyelembevételével történik.

2. Az irányadó jog a lengyel jog.

3. A nyelvi verziók közötti eltérés esetén a lengyel verzió az irányadó.

11. Hatálybalépés

A Biztonsági Szabályzat jelen verziója **2026-03-05** napjától hatályos.

A dokumentum aktuális verziója a Safety Software szolgáltatásban kerül közzétételre.

Adatkezelő és a rendszer tulajdonosa:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polska
E-mail: **office@safetysoftware.eu**

Változásnapló

Frissítés: 2026-03-05

- pontosítottuk a rétegzett biztonsági mentéseket és az adat-helyreállítási folyamatot (BCP/DR)
- kiegészítettük az adattitkosítás leírását a borítékmodellel és a külső kulcskezeléssel
- bővítettük az alkalmazásszintű védelem leírását munkamenetekkel, CSRF-fel, CSP-vel és visszaélés-ellenes mechanizmusokkal
- hozzáadtuk a monitorozás és riasztások szekcióját, valamint egyszerűsítettük a külső szolgáltatásokkal való integráció szekcióját