Политика за сигурност

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

Политика за сигурност на приложението Safety Software (SaaS)

ID: SE-2026-V2
Актуализация: 2026-03-05

1. Цел и обхват

Настоящата Политика за сигурност определя правилата за защита на информацията и данните, обработвани в рамките на приложението Safety Software, предоставяно по модела Software as a Service (SaaS).

Документът се отнася до сигурността на потребителите, използващи приложението в услугата Safety Software, и представлява допълнение към Общите условия и Политиката за поверителност.

Политиката има информационен характер и описва основните технически и организационни мерки, прилагани от Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polska (наричан по-долу: „Администратор“).

2. Модел на отговорност

Системата работи по модел на споделена отговорност:

1. **Администраторът (Safety Software)** отговаря за сигурността на кода на приложението, механизмите за вход, авторизация и сесии, защитата на данните на приложно ниво, извършването на резервни копия, както и реакцията при инциденти със сигурността.

2. **Доставчиците на инфраструктура и помощни услуги** отговарят за сигурността на елементите, които попадат в обхвата на предоставяните от тях услуги.

3. **Клиентът** отговаря за сигурността на своите устройства, пароли, идентичностите на потребителите, както и управлението на достъпите в своя екип.

3. Правила за сигурност на приложението

1. Предаването на данни се осъществява изключително с използване на TLS криптиране.

2. Потребителските сесии са защитени чрез „бисквитки“ с атрибути **HttpOnly**, **Secure** (за криптирани връзки) и **SameSite**. След удостоверяване се извършва ротация на идентификатора на сесията.

3. За сесиите се прилагат лимити за неактивност и за максимална продължителност.

4. Заявките, които променят състоянието на системата, са защитени с CSRF токени, валидирани от страна на сървъра.

5. Приложението прилага рестриктивна политика за сигурност на съдържанието, включително механизми, ограничаващи изпълнението на неоторизирани скриптове, както и стандартни заглавки за сигурност на браузъра.

6. Прилагат се механизми за ограничаване на злоупотреби, включително rate limiting и защита срещу опити за вход чрез brute force.

7. Всяка операция се изпълнява в контекста на потребител и организация; неоторизираният достъп се блокира.

4. Криптиране и защита на данните

1. Потребителските пароли се съхраняват с използване на алгоритъма **bcrypt**.

2. Избрани чувствителни данни, съхранявани в базата, са защитени с използване на модел на пликово криптиране на данни. Криптографските ключове се управляват отделно във външна система за управление на ключове.

3. Когато е обосновано, се прилагат механизми, ограничаващи експозицията на данни при запазване на функциите за търсене или идентификация, без необходимост от съхраняване на пълните стойности в открит вид.

5. Резервни копия и възстановяване (BCP/DR)

1. Прилагаме слоест подход към резервните копия: локални копия за бързо възстановяване и копия, съхранявани извън основната среда.

2. Копията, съхранявани извън основната среда, включват образи на средата, изготвяни инкрементално. Те са криптирани, редовно валидирани и обхванати от тестове за възстановяване.

3. Базата данни се защитава чрез приложно консистентни копия. Допълнително се поддържат локални дъмпове на базата, подпомагащи бързото възстановяване.

4. Цялостта на копията се проверява с използване на контролни механизми, включително контролни суми.

5. Процесът на изготвяне на копия е автоматизиран, изпълнява се ежедневно и се наблюдава по отношение на успешното и неуспешното изпълнение на задачите.

6. Редовно се провеждат тестове за възстановяване на данни, включващи поне възстановяване на избрани файлове.

6. Мониторинг и известия

1. Системата регистрира избрани събития по сигурността и административни операции, в частност свързани с удостоверяване, опити за достъп и работата на критични процеси.

2. Прилагат се механизми за мониторинг и автоматични известия при неуспех на задачи, критични грешки и събития, които могат да указват злоупотреба или инцидент със сигурността.

3. Достъпът до логове и оперативна информация е ограничен до упълномощени лица.

7. Инфраструктура и поддържане на сигурността

1. Административният достъп е ограничен до упълномощени лица и е защитен с механизми за силно удостоверяване, включително удостоверяване с ключове.

2. Директният вход в привилегирован акаунт е изключен или ограничен съгласно принципа на минималните привилегии.

3. Прилагат се механизми за филтриране на трафика, защита срещу опити за достъп чрез brute force и мониторинг на инфраструктурни събития.

4. Актуализациите по сигурността се внедряват регулярно.

5. Пощенските услуги, използвани за обслужване на системата, са защитени чрез криптиране на преноса и механизми, ограничаващи злоупотреби.

8. Доставчици и интеграции

1. Доколкото системата използва външни услуги или помощни интеграции, подборът на решения отчита сигурността на данните, принципа на минимизация и контрола на обхвата на предаваната информация.

2. Комуникацията с външни услуги се осъществява с използване на криптиран пренос.

9. Докладване на инциденти

Сигнали относно сигурността на приложението или съмнения за инциденти следва да се изпращат на адрес:

office@safetysoftware.eu
Тема на съобщението: SECURITY

Сигналите се анализират съгласно вътрешната процедура за обработка на инциденти.

10. Съответствие и юрисдикция

1. Мерките за сигурност се проектират и поддържат с оглед на действащите правни разпоредби, включително изискванията на **GDPR**, както и признатите практики за информационна сигурност.

2. Приложимото право е полското право.

3. В случай на разминавания между езиковите версии, решаваща е полската версия.

11. Влизане в сила

Настоящата версия на Политиката за сигурност е в сила от **2026-03-05**.

Актуалната версия на документа е публикувана в услугата Safety Software.

Администратор на данните и собственик на системата:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polska
E-mail: **office@safetysoftware.eu**

Дневник на промените

Актуализация: 2026-03-05

- уточнени са слоестите резервни копия и процесът на възстановяване на данни (BCP/DR)

- допълнено е описанието на криптирането на данни с envelope модел и външно управление на ключове

- разширено е описанието на защитата на приложението със сесии, CSRF, CSP и антизлоупотребни механизми

- добавена е секция за мониторинг и предупреждения (alerts), както и опростена секция за интеграция с външни услуги