Politique de sécurité

<?xml encoding="utf-8" ?>

Politique de sécurité de l’application Safety Software (SaaS)

ID: SE-2026-V2
Mise à jour : 2026-03-05

1. Objet et portée

La présente Politique de sécurité définit les principes de protection des informations et des données traitées dans le cadre de l’application Safety Software mise à disposition selon le modèle Software as a Service (SaaS).

Le document concerne la sécurité des utilisateurs utilisant l’application dans le service Safety Software et constitue un complément aux Conditions générales ainsi qu’à la Politique de confidentialité.

La Politique a un caractère informatif et décrit les mesures techniques et organisationnelles de base appliquées par Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Cracovie, Pologne (ci-après : « Administrateur »).

2. Modèle de responsabilité

Le système fonctionne selon un modèle de responsabilité partagée :

1. **Administrateur (Safety Software)** est responsable de la sécurité du code de l’application, des mécanismes de connexion, d’autorisation et de session, de la protection des données au niveau applicatif, de l’exécution des sauvegardes ainsi que de la réponse aux incidents de sécurité.

2. **Fournisseurs d’infrastructure et de services auxiliaires** sont responsables de la sécurité des éléments relevant du périmètre des services qu’ils fournissent.

3. **Client** est responsable de la sécurité de ses appareils, de ses mots de passe, des identités des utilisateurs ainsi que de la gestion des accès au sein de son équipe.

3. Principes de sécurité de l’application

1. La transmission des données s’effectue exclusivement au moyen du chiffrement TLS.

2. Les sessions des utilisateurs sont sécurisées au moyen de cookies avec les attributs **HttpOnly**, **Secure** (pour les connexions chiffrées) ainsi que **SameSite**. Après l’authentification, une rotation de l’identifiant de session est effectuée.

3. Des limites d’inactivité ainsi que de durée maximale sont appliquées aux sessions.

4. Les requêtes modifiant l’état du système sont protégées par des jetons CSRF vérifiés côté serveur.

5. L’application applique une politique de sécurité du contenu stricte, incluant des mécanismes limitant l’exécution de scripts non autorisés ainsi que des en-têtes de sécurité standard du navigateur.

6. Des mécanismes limitant les abus sont appliqués, notamment le rate limiting ainsi que la protection contre les tentatives de connexion par force brute.

7. Chaque opération est effectuée dans le contexte de l’utilisateur et de l’organisation ; l’accès non autorisé est bloqué.

4. Chiffrement et protection des données

1. Les mots de passe des utilisateurs sont stockés à l’aide de l’algorithme **bcrypt**.

2. Certaines données sensibles stockées dans la base sont protégées au moyen d’un modèle de chiffrement des données par enveloppe. Les clés cryptographiques sont gérées séparément dans un système externe de gestion des clés.

3. Là où cela est justifié, des mécanismes limitant l’exposition des données sont appliqués tout en conservant les fonctions de recherche ou d’identification, sans nécessité de stocker les valeurs complètes en clair.

5. Sauvegarde et restauration (BCP/DR)

1. Nous appliquons une approche en couches des sauvegardes : des copies locales pour une restauration rapide ainsi que des copies conservées hors de l’environnement principal.

2. Les copies conservées hors de l’environnement principal incluent des images d’environnement réalisées de manière incrémentale. Elles sont chiffrées, validées régulièrement et soumises à des tests de restauration.

3. La base de données est protégée par des copies cohérentes au niveau applicatif. En outre, des dumps locaux de la base sont maintenus afin de faciliter une restauration rapide.

4. L’intégrité des copies est vérifiée à l’aide de mécanismes de contrôle, notamment des sommes de contrôle.

5. Le processus de sauvegarde est automatisé, exécuté quotidiennement et fait l’objet d’une surveillance des succès et des échecs des tâches.

6. Des tests réguliers de restauration des données sont effectués, incluant au minimum la restauration de fichiers sélectionnés.

6. Supervision et alertes

1. Le système enregistre certains événements de sécurité ainsi que des opérations administratives, en particulier ceux liés à l’authentification, aux tentatives d’accès et au fonctionnement des processus critiques.

2. Des mécanismes de supervision ainsi que des alertes automatiques en cas d’échec de tâches, d’erreurs critiques et d’événements pouvant indiquer un abus ou un incident de sécurité sont appliqués.

3. L’accès aux logs et aux informations opérationnelles est limité aux personnes autorisées.

7. Infrastructure et maintien de la sécurité

1. L’accès administratif est limité aux personnes autorisées et sécurisé par des mécanismes d’authentification forte, y compris l’authentification par clés.

2. La connexion directe à un compte privilégié est désactivée ou limitée conformément au principe du moindre privilège.

3. Des mécanismes de filtrage du trafic, de protection contre les tentatives d’accès par force brute ainsi que de surveillance des événements d’infrastructure sont appliqués.

4. Les mises à jour de sécurité sont déployées régulièrement.

5. Les services de messagerie utilisés pour l’exploitation du système sont sécurisés par le chiffrement de la transmission ainsi que par des mécanismes limitant les abus.

8. Fournisseurs et intégrations

1. Dans la mesure où le système utilise des services externes ou des intégrations auxiliaires, le choix des solutions tient compte de la sécurité des données, du principe de minimisation ainsi que du contrôle du périmètre des informations transmises.

2. La communication avec les services externes s’effectue au moyen d’une transmission chiffrée.

9. Signalement des incidents

Les signalements concernant la sécurité de l’application ou les soupçons d’incidents doivent être adressés à :

office@safetysoftware.eu
Objet du message : SECURITY

Les signalements sont analysés conformément à la procédure interne de gestion des incidents.

10. Conformité et juridiction

1. Les mesures de sécurité sont conçues et maintenues en tenant compte des dispositions légales applicables, y compris des exigences du **RGPD**, ainsi que des pratiques reconnues de sécurité de l’information.

2. Le droit applicable est le droit polonais.

3. En cas de divergence entre les versions linguistiques, la version polonaise fait foi.

11. Entrée en vigueur

La présente version de la Politique de Sécurité est en vigueur à compter du **2026-03-05**.

La version actuelle du document est publiée sur le service Safety Software.

Administrateur des données et propriétaire du système :
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Pologne
E-mail : **office@safetysoftware.eu**

Journal des modifications

Mise à jour : 2026-03-05

- les sauvegardes multicouches ainsi que le processus de restauration des données (BCP/DR) ont été précisés

- la description du chiffrement des données a été complétée avec le modèle enveloppe et la gestion externe des clés

- la description de la protection applicative a été étendue aux sessions, CSRF, CSP et aux mécanismes anti-abus

- une section sur la surveillance et les alertes a été ajoutée et la section sur l’intégration avec des services externes a été simplifiée