Πολιτική Ασφάλειας

Πολιτική Ασφάλειας της Εφαρμογής Safety Software (SaaS)

ID: SE-2026-V2
Ενημέρωση: 2026-03-05

1. Σκοπός και πεδίο εφαρμογής

Η παρούσα Πολιτική Ασφάλειας καθορίζει τους κανόνες προστασίας πληροφοριών και δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο της εφαρμογής Safety Software που διατίθεται στο μοντέλο Software as a Service (SaaS).

Το έγγραφο αφορά την ασφάλεια των χρηστών που χρησιμοποιούν την εφαρμογή στην υπηρεσία Safety Software και αποτελεί συμπλήρωμα των Όρων Χρήσης και της Πολιτικής Απορρήτου.

Η Πολιτική έχει ενημερωτικό χαρακτήρα και περιγράφει τα βασικά τεχνικά και οργανωτικά μέτρα που εφαρμόζει η Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polska (εφεξής: «Διαχειριστής»).

2. Μοντέλο ευθύνης

Το σύστημα λειτουργεί με μοντέλο επιμερισμένης ευθύνης:

1. **Ο Διαχειριστής (Safety Software)** είναι υπεύθυνος για την ασφάλεια του κώδικα της εφαρμογής, τους μηχανισμούς σύνδεσης, εξουσιοδότησης και συνεδρίας, την προστασία δεδομένων στο επίπεδο εφαρμογής, τη δημιουργία αντιγράφων ασφαλείας και την αντιμετώπιση περιστατικών ασφάλειας.

2. **Οι πάροχοι υποδομής και βοηθητικών υπηρεσιών** είναι υπεύθυνοι για την ασφάλεια των στοιχείων που εμπίπτουν στο πεδίο των υπηρεσιών που παρέχουν.

3. **Ο Πελάτης** είναι υπεύθυνος για την ασφάλεια των συσκευών του, των κωδικών πρόσβασης, των ταυτοτήτων χρηστών και για τη διαχείριση προσβάσεων στην ομάδα του.

3. Κανόνες ασφάλειας εφαρμογής

1. Η μετάδοση δεδομένων πραγματοποιείται αποκλειστικά με χρήση κρυπτογράφησης TLS.

2. Οι συνεδρίες χρηστών προστατεύονται με χρήση cookies με τα χαρακτηριστικά **HttpOnly**, **Secure** (για κρυπτογραφημένες συνδέσεις) και **SameSite**. Μετά την αυθεντικοποίηση πραγματοποιείται εναλλαγή (rotation) του αναγνωριστικού συνεδρίας.

3. Για τις συνεδρίες εφαρμόζονται όρια αδράνειας και μέγιστης διάρκειας.

4. Τα αιτήματα που μεταβάλλουν την κατάσταση του συστήματος προστατεύονται με tokens CSRF που επαληθεύονται στην πλευρά του διακομιστή.

5. Η εφαρμογή εφαρμόζει αυστηρή πολιτική ασφάλειας περιεχομένου, συμπεριλαμβανομένων μηχανισμών που περιορίζουν την εκτέλεση μη εξουσιοδοτημένων scripts και των τυπικών headers ασφάλειας του προγράμματος περιήγησης.

6. Εφαρμόζονται μηχανισμοί περιορισμού καταχρήσεων, συμπεριλαμβανομένων rate limiting και προστασίας από προσπάθειες σύνδεσης με χρήση ωμής βίας.

7. Κάθε λειτουργία εκτελείται στο πλαίσιο χρήστη και οργανισμού· η μη εξουσιοδοτημένη πρόσβαση αποκλείεται.

4. Κρυπτογράφηση και προστασία δεδομένων

1. Οι κωδικοί πρόσβασης των χρηστών αποθηκεύονται με χρήση του αλγορίθμου **bcrypt**.

2. Επιλεγμένα ευαίσθητα δεδομένα που αποθηκεύονται στη βάση προστατεύονται με χρήση μοντέλου envelope encryption. Τα κρυπτογραφικά κλειδιά διαχειρίζονται ξεχωριστά σε εξωτερικό σύστημα διαχείρισης κλειδιών.

3. Όπου αυτό είναι αιτιολογημένο, εφαρμόζονται μηχανισμοί που περιορίζουν την έκθεση δεδομένων, διατηρώντας τη λειτουργία αναζήτησης ή ταυτοποίησης, χωρίς να απαιτείται η αποθήκευση πλήρων τιμών σε απλή μορφή.

5. Backup και αποκατάσταση (BCP/DR)

1. Εφαρμόζουμε πολυεπίπεδη προσέγγιση για τα αντίγραφα ασφαλείας: τοπικά αντίγραφα για γρήγορη αποκατάσταση και αντίγραφα που τηρούνται εκτός του βασικού περιβάλλοντος.

2. Τα αντίγραφα που τηρούνται εκτός του βασικού περιβάλλοντος περιλαμβάνουν images περιβάλλοντος που λαμβάνονται αυξητικά. Είναι κρυπτογραφημένα, επαληθεύονται τακτικά και υπόκεινται σε δοκιμές αποκατάστασης.

3. Η βάση δεδομένων προστατεύεται με application-consistent αντίγραφα. Επιπλέον, διατηρούνται τοπικά dumps της βάσης που υποστηρίζουν γρήγορη αποκατάσταση.

4. Η ακεραιότητα των αντιγράφων επαληθεύεται με χρήση μηχανισμών ελέγχου, συμπεριλαμβανομένων checksums.

5. Η διαδικασία δημιουργίας αντιγράφων είναι αυτοματοποιημένη, εκτελείται καθημερινά και παρακολουθείται ως προς την επιτυχία και αποτυχία των εργασιών.

6. Διενεργούνται τακτικά δοκιμές αποκατάστασης δεδομένων, που περιλαμβάνουν τουλάχιστον την αποκατάσταση επιλεγμένων αρχείων.

6. Παρακολούθηση και ειδοποιήσεις

1. Το σύστημα καταγράφει επιλεγμένα συμβάντα ασφάλειας και διοικητικές λειτουργίες, ιδίως εκείνες που σχετίζονται με αυθεντικοποίηση, προσπάθειες πρόσβασης και λειτουργία κρίσιμων διεργασιών.

2. Εφαρμόζονται μηχανισμοί παρακολούθησης και αυτόματες ειδοποιήσεις για αποτυχία εργασιών, κρίσιμα σφάλματα και συμβάντα που μπορεί να υποδεικνύουν κατάχρηση ή περιστατικό ασφάλειας.

3. Η πρόσβαση σε logs και λειτουργικές πληροφορίες περιορίζεται σε εξουσιοδοτημένα άτομα.

7. Υποδομή και διατήρηση της ασφάλειας

1. Η διαχειριστική πρόσβαση περιορίζεται σε εξουσιοδοτημένα άτομα και προστατεύεται με μηχανισμούς ισχυρής αυθεντικοποίησης, συμπεριλαμβανομένης της αυθεντικοποίησης με κλειδιά.

2. Η απευθείας σύνδεση σε προνομιούχο λογαριασμό είναι απενεργοποιημένη ή περιορισμένη σύμφωνα με την αρχή των ελάχιστων δικαιωμάτων.

3. Εφαρμόζονται μηχανισμοί φιλτραρίσματος κίνησης, προστασίας από προσπάθειες πρόσβασης με χρήση ωμής βίας και παρακολούθησης συμβάντων υποδομής.

4. Οι ενημερώσεις ασφάλειας εφαρμόζονται τακτικά.

5. Οι υπηρεσίες ηλεκτρονικού ταχυδρομείου που χρησιμοποιούνται για την υποστήριξη του συστήματος προστατεύονται με κρυπτογράφηση μετάδοσης και με μηχανισμούς περιορισμού καταχρήσεων.

8. Πάροχοι και ενσωματώσεις

1. Στο μέτρο που το σύστημα χρησιμοποιεί εξωτερικές υπηρεσίες ή βοηθητικές ενσωματώσεις, η επιλογή λύσεων λαμβάνει υπόψη την ασφάλεια δεδομένων, την αρχή της ελαχιστοποίησης και τον έλεγχο του εύρους των πληροφοριών που διαβιβάζονται.

2. Η επικοινωνία με εξωτερικές υπηρεσίες πραγματοποιείται με χρήση κρυπτογραφημένης μετάδοσης.

9. Αναφορά περιστατικών

Οι αναφορές σχετικά με την ασφάλεια της εφαρμογής ή υποψίες περιστατικών πρέπει να αποστέλλονται στη διεύθυνση:

office@safetysoftware.eu
Θέμα μηνύματος: SECURITY

Οι αναφορές αναλύονται σύμφωνα με την εσωτερική διαδικασία χειρισμού περιστατικών.

10. Συμμόρφωση και δικαιοδοσία

1. Τα μέτρα ασφάλειας σχεδιάζονται και διατηρούνται λαμβάνοντας υπόψη τις ισχύουσες νομικές διατάξεις, συμπεριλαμβανομένων των απαιτήσεων του **ΓΚΠΔ**, καθώς και αναγνωρισμένων πρακτικών ασφάλειας πληροφοριών.

2. Εφαρμοστέο δίκαιο είναι το πολωνικό δίκαιο.

3. Σε περίπτωση αποκλίσεων μεταξύ γλωσσικών εκδόσεων, υπερισχύει η πολωνική έκδοση.

11. Έναρξη ισχύος

Η παρούσα έκδοση της Πολιτικής Ασφάλειας ισχύει από την ημερομηνία **2026-03-05**.

Η τρέχουσα έκδοση του εγγράφου δημοσιεύεται στην υπηρεσία Safety Software.

Υπεύθυνος επεξεργασίας δεδομένων και ιδιοκτήτης του συστήματος:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polska
E-mail: **office@safetysoftware.eu**

Αρχείο αλλαγών

Ενημέρωση: 2026-03-05

- διευκρινίστηκαν τα πολυεπίπεδα αντίγραφα ασφαλείας και η διαδικασία αποκατάστασης δεδομένων (BCP/DR)
- συμπληρώθηκε η περιγραφή της κρυπτογράφησης δεδομένων με το μοντέλο φακέλου (envelope) και την εξωτερική διαχείριση κλειδιών
- επεκτάθηκε η περιγραφή της προστασίας σε επίπεδο εφαρμογής με συνεδρίες, CSRF, CSP και μηχανισμούς κατάχρησης
- προστέθηκε ενότητα παρακολούθησης και ειδοποιήσεων και απλοποιήθηκε η ενότητα ενσωμάτωσης με εξωτερικές υπηρεσίες