Drošības politika

Safety Software | Aktualizacja: 03.09.2026 | https://safetysoftware.eu

Safety Software (SaaS) lietojumprogrammas drošības politika

ID: SE-2026-V2
Atjaunināj ums: 2026-03-05

1. Mērķis un darbības joma

Šī Drošības politika nosaka informācijas un datu aizsardzības noteikumus, kas tiek apstrādāti Safety Software lietojumprogrammā, kura tiek nodrošināta Software as a Service (SaaS) modelī.

Dokuments attiecas uz to lietotāju drošību, kuri izmanto lietojumprogrammu Safety Software servisā, un tas papildina Noteikumus un Privātuma politiku.

Politikai ir informatīvs raksturs, un tajā aprakstīti Safety Software Sp. z o.o., ul. Półłanki 80, 30-740 Kraków, Polska (turpmāk: “Administrators”) piemērotie pamata tehniskie un organizatoriskie pasākumi.

2. Atbildības modelis

Sistēma darbojas kopīgās atbildības modelī:

1. **Administrators (Safety Software)** atbild par lietojumprogrammas koda drošību, pieteikšanās, autorizācijas un sesiju mehānismiem, datu aizsardzību lietojumprogrammas slānī, rezerves kopiju izveidi un reaģēšanu uz drošības incidentiem.

2. **Infrastruktūras un palīgpakalpojumu piegādātāji** atbild par to elementu drošību, kas ietilpst viņu sniegto pakalpojumu apjomā.

3. **Klients** atbild par savu ierīču, paroļu, lietotāju identitāšu drošību, kā arī piekļuves pārvaldību savā komandā.

3. Lietojumprogrammas drošības principi

1. Datu pārraide notiek tikai, izmantojot TLS šifrēšanu.

2. Lietotāju sesijas tiek aizsargātas, izmantojot sīkdatnes ar atribūtiem **HttpOnly**, **Secure** (šifrētiem savienojumiem) un **SameSite**. Pēc autentifikācijas notiek sesijas identifikatora rotācija.

3. Sesijām tiek piemēroti dīkstāves un maksimālā darbības ilguma limiti.

4. Pieprasījumi, kas maina sistēmas stāvokli, tiek aizsargāti ar CSRF tokeniem, kas tiek verificēti servera pusē.

5. Lietojumprogramma izmanto stingru satura drošības politiku, tostarp mehānismus, kas ierobežo neautorizētu skriptu izpildi, kā arī standarta pārlūkprogrammas drošības galvenes.

6. Tiek izmantoti mehānismi ļaunprātīgas izmantošanas ierobežošanai, tostarp rate limiting un aizsardzība pret brutāla spēka pieteikšanās mēģinājumiem.

7. Katra darbība tiek veikta lietotāja un organizācijas kontekstā; neautorizēta piekļuve tiek bloķēta.

4. Šifrēšana un datu aizsardzība

1. Lietotāju paroles tiek glabātas, izmantojot **bcrypt** algoritmu.

2. Atlasīti sensitīvi dati, kas tiek glabāti datubāzē, ir aizsargāti, izmantojot aploksnes datu šifrēšanas modeli. Kriptogrāfiskās atslēgas tiek pārvaldītas atsevišķi ārējā atslēgu pārvaldības sistēmā.

3. Tur, kur tas ir pamatoti, tiek izmantoti mehānismi, kas ierobežo datu ekspozīciju, saglabājot meklēšanas vai identifikācijas funkcijas, bez nepieciešamības glabāt pilnās vērtības atklātā veidā.

5. Rezerves kopēšana un atjaunošana (BCP/DR)

1. Mēs izmantojam slāņainu pieeju rezerves kopijām: lokālās kopijas ātrai atjaunošanai un kopijas, kas tiek glabātas ārpus primārās vides.

2. Kopijas, kas tiek glabātas ārpus primārās vides, ietver vides attēlus, kas tiek veidoti inkrementāli. Tie tiek šifrēti, regulāri validēti un iekļauti atjaunošanas testos.

3. Datubāze tiek aizsargāta ar lietojumprogrammas līmenī konsistentām kopijām. Papildus tiek uzturēti lokāli datubāzes izgāztuves faili, kas atbalsta ātru atjaunošanu.

4. Kopiju integritāte tiek pārbaudīta, izmantojot kontroles mehānismus, tostarp kontrolsummas.

5. Kopēšanas process ir automatizēts, tiek veikts katru dienu un tiek uzraudzīts attiecībā uz uzdevumu izpildes sekmēm un neveiksmēm.

6. Regulāri tiek veikti datu atjaunošanas testi, kas ietver vismaz atlasītu failu atjaunošanu.

6. Uzraudzība un brīdinājumi

1. Sistēma reģistrē atlasītus drošības notikumus un administratīvās darbības, jo īpaši saistībā ar autentifikāciju, piekļuves mēģinājumiem un kritisko procesu darbību.

2. Tiek izmantoti uzraudzības mehānismi un automātiski brīdinājumi par uzdevumu neveiksmēm, kritiskām kļūdām un notikumiem, kas var norādīt uz ļaunprātīgu izmantošanu vai drošības incidentu.

3. Piekļuve žurnāliem un operatīvajai informācijai ir ierobežota līdz pilnvarotām personām.

7. Infrastruktūra un drošības uzturēšana

1. Administratīvā piekļuve ir ierobežota līdz pilnvarotām personām un aizsargāta ar spēcīgas autentifikācijas mehānismiem, tostarp autentifikāciju ar atslēgām.

2. Tiešā pieteikšanās priviliģētā kontā ir atslēgta vai ierobežota saskaņā ar minimālo privilēģiju principu.

3. Tiek izmantoti satiksmes filtrēšanas mehānismi, aizsardzība pret brutāla spēka piekļuves mēģinājumiem un infrastruktūras notikumu uzraudzība.

4. Drošības atjauninājumi tiek ieviesti regulāri.

5. Pasta pakalpojumi, kas tiek izmantoti sistēmas apkalpošanai, ir aizsargāti ar pārraides šifrēšanu un mehānismiem, kas ierobežo ļaunprātīgu izmantošanu.

8. Piegādātāji un integrācijas

1. Tādā apmērā, kādā sistēma izmanto ārējos pakalpojumus vai palīgintegrācijas, risinājumu izvēlē tiek ņemta vērā datu drošība, minimizācijas princips un nododamās informācijas apjoma kontrole.

2. Saziņa ar ārējiem pakalpojumiem notiek, izmantojot šifrētu pārraidi.

9. Incidentu ziņošana

Paziņojumi par lietojumprogrammas drošību vai aizdomām par incidentiem jānosūta uz adresi:

office@safetysoftware.eu
Ziņojuma temats: SECURITY

Paziņojumi tiek analizēti saskaņā ar iekšējo incidentu apstrādes procedūru.

10. Atbilstība un jurisdikcija

1. Drošības pasākumi tiek projektēti un uzturēti, ievērojot piemērojamos tiesību aktus, tostarp **VDAR** prasības, kā arī atzītas informācijas drošības prakses.

2. Piemērojamās tiesības ir Polijas tiesības.

3. Ja pastāv neatbilstības starp valodu versijām, noteicošā ir poļu valodas versija.

11. Stāšanās spēkā

Šī Drošības politikas versija ir spēkā no **2026-03-05**.

Dokumenta aktuālā versija tiek publicēta Safety Software servisā.

Datu pārzinis un sistēmas īpašnieks:
Safety Software Sp. z o.o.
ul. Półłanki 80
30-740 Kraków, Polija
E-pasts: **office@safetysoftware.eu**

Izmaiņu žurnāls

Atjauninājums: 2026-03-05

- precizētas slāņveida rezerves kopijas un datu atjaunošanas process (BCP/DR)
- papildināts datu šifrēšanas apraksts ar aploksnes modeli un ārēju atslēgu pārvaldību
- paplašināts lietojumprogrammu aizsardzības apraksts, iekļaujot sesijas, CSRF, CSP un pretļaunprātīgas izmantošanas mehānismus
- pievienota monitoringa un brīdinājumu sadaļa, kā arī vienkāršota integrācijas ar ārējiem pakalpojumiem sadaļa