sosafe

Veiligheid en Vertrouwen

SoSafe's beveiligingsaanpak

Index

Zo gaan wij om met beveiliging

In dit deel gaan we in op hoe SoSafe omgaat met beveiliging. We behandelen de belangrijkste stappen die we nemen en de controles die we implementeren in verschillende beveiligingsdomeinen. Zowel bij het beveiligen van onze eigen omgevingen (inclusief ons cloudgebaseerde platform) als de processen die we hanteren om ervoor te zorgen dat we producten creëren die zo veilig mogelijk zijn voor onze klanten en gebruikers.

Motivatie die ten grondslag ligt aan onze beveiliging

Beveiliging heeft bij ons een zeer hoge prioriteit. We leveren een informatie-beveiligingsproduct aan onze klanten, dus streven we ernaar ook een hoog niveau van beveiliging voor onszelf te handhaven.

Hoe meer we groeien, hoe meer klanten ons product zullen gebruiken. Onze behoefte aan sterke en geavanceerde beveiliging zal in de toekomst dus nog verder toenemen.

Het succes van SoSafe GmbH is voor een groot deel afhankelijk van het feit dat onze bedrijfsinformatie en klantinformatie, actueel en ongewijzigd zijn en met de vereiste vertrouwelijkheid worden behandeld.

Ons team

We hebben professionals ingehuurd op verschillende gebieden van beveiliging om te voldoen aan onze zeer ambitieuze beveiligingseisen – en we blijven op zoek naar gekwalificeerde professionals om een state-of-the-art beveiligingsstructuur bij SoSafe neer te zetten, te onderhouden en te verbeteren. We streven ernaar best-in-class te zijn op het gebied van beveiliging. Daarom bestaat ons team voor beveiliging uit de volgende rollen:

- **CISO** - Geeft leiding aan beveiligingsinitiatieven binnen SoSafe; verantwoordelijk voor het monitoren en handhaven van de beveiliging van SoSafe door ervoor te zorgen dat alle rollen op het vlak van beveiliging goed samenwerken.
- **Hoofd Informatiebeveiliging** - Verantwoordelijk voor het continu ontwikkelen van geavanceerde informatiebeveiligingsprocessen, risicomanagement en kaders voor compliance en governance.
- **Informatiebeveiligingsmanager -** Verantwoordelijk voor informatie-beveiligingsprocessen en -monitoring, inclusief de naleving van sectorspecifieke regelgeving, certificering en het operationeel houden van ons ISMS.
- **Applicatiebeveiliging** - Verantwoordelijk voor de beveiliging van onze producten en platforms.

- **SOC Team** - Verantwoordelijk voor incidentbeheer en monitoringstests, voorspellende aanvalsanalyse en het verzamelen van dreigingsinformatie.
- **Juridisch** - Verantwoordelijk voor naleving van wettelijke vereisten en certificeringen.
- **Functionaris voor gegevensbescherming** - Verantwoordelijk voor het waarborgen van algehele AVG-naleving voor alle verwerkingsactiviteiten van persoonsgegevens door SoSafe.

Naast ons gespecialiseerde team voltooien alle medewerkers bij SoSafe onze e-learning over beveiliging en zijn ze goed getraind om aan onze eisen voor beveiliging te voldoen.

Beoordelingen door derden

ISO 27001

Als bedrijf hebben we de ISO 27001-audit afgerond en zijn we sinds 20 december 2022 ISO 27001-gecertificeerd en ondergaan jaarlijks performance surveillance audits. We streven ernaar om regelmatig audits te ondergaan van onafhankelijke derde partijen, die zelf ook regelmatig SOC 1-, SOC 2- en/of ISO/IEC 27001-audits ondergaan om hun werkwijzen te verifiëren.

Download ISO certificaat →

TISAX®

Bij SoSafe erkennen we het belang van het handhaven van de hoogste mate van vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Om de hoogste normen voor beveiliging te waarborgen, nemen we deel aan de Trusted Information Security Assessment Exchange (TISAX®), gefaciliteerd door de ENX Association namens de Duitse Vereniging van de Automobielindustrie (VDA).

TISAX®-beoordelingen worden uitgevoerd door gekwalificeerde auditproviders die regelmatig kwalificatiebeoordelingen ondergaan. Het is belangrijk op te merken dat de resultaten van TISAX®-beoordelingen niet zijn bedoeld voor het grote publiek. Om exclusieve toegang te krijgen tot de resultaten van onze beoordeling, kun je het ENX-portaal bezoeken via: TISAX Assessment Resultaten ENX Portal. Onze resultaten zijn beschikbaar onder de beoordelings-ID ACMGNV en Scope-ID S02C8M.

Beveiligen van interne bedrijfs-activiteiten

Een effectieve aanpak van beveiliging begint met het handhaven van de veiligheid van onze interne omgevingen. Onze interne beveiligingsstrategie omvat de volgende beveiligingsprincipes:

Toegangsbeheer

In onze toepassingscontext verwijst 'Toegang' naar het gebruik van IT-systemen, systeemonderdelen, netwerken en het gebruik van informatie.

De uitgangspunten voor algemeen toegangsbeheer zijn onder meer:

- **Need-to-know principe:**
  Medewerkers van SoSafe krijgen alleen de rechten of privileges die absoluut noodzakelijk zijn voor het vervullen van hun taken. Administratieve privileges worden op zeer beperkte schaal verleend.

- **Principe van minste privileges:**
  Gebruikers krijgen alleen de rechten en privileges die absoluut noodzakelijk zijn om hun taken uit te voeren.

- **Scheiding van taken en principe van dubbele controle:**
  Bij het toekennen van gebruikersrechten moet rekening worden gehouden met de scheiding van taken en/of het controleprincipe met betrekking tot tegenstrijdige taken.

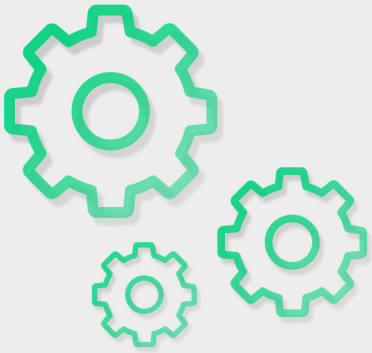
- **Gebruikersbeheer:**
  Het beheer van gebruikers, groepen en machtigingen is gecentraliseerd met behulp van technieken zoals Single Sign-On (SSO) om het aantal te onderhouden gebruikersdirectories te minimaliseren.

- **Toekenning, aanpassing en intrekking van rechten:**
  Het aanpassen van toegangsrechten wordt uitgevoerd volgens het 'vier-ogen'-principe. Als een gebruikersrecht buiten de toestemmingen-baseline wordt toegekend, moet dit worden gedocumenteerd. We werken met dubbele goedkeuring voor administratieve toegang, wat betekent dat deze moet worden goedgekeurd door de asset-eigenaar en een supervisor.

  Alle toegangsrechten worden ook minimaal een keer per jaar gecontroleerd. Administratieve toegang wordt minimaal om de zes maanden gecontroleerd volgens ons toegangsbeheerbeleid of bij een relevante wijziging van een asset.

  Als onderdeel van de principes van de need-to-know en minste privileges worden inactieve accounts dienovereenkomstig geblokkeerd of verwijderd.

  Ten slotte worden alle toegangsrechten na het vertrek van een werknemer binnen 24 uur ingetrokken.



- **Toegang tot broncode:**
  Toegang tot de broncode of de code-repository is beperkt om te voorkomen dat onbevoegde personen toegang krijgen en om mogelijke openbaarmaking van bedrijfsgeheimen te voorkomen. De principes van de need-to-know en minste privileges moeten altijd zoveel mogelijk worden gevolgd. Er wordt bijzondere aandacht besteed aan tijdelijke medewerkers, zoals werkstudenten, stagiairs of externe ontwikkelaars.

- **Authenticatievereisten**
  Een account wordt geblokkeerd na zes mislukte pogingen.

  Externe toegang vanuit openbare externe netwerkzones is alleen mogelijk met behulp van de bedrijfs-VPN die de informatie tijdens de overdracht versleutelt en toegankelijk is via tweestapsverificatie (2FA).

Beveiliging van endpoint-apparaten

Alle endpoint-apparaten zijn beveiligd met endpoint-bescherming, evenals onze bestandsopslag- en -uitwisselingsplatforms.

Alle medewerkers van SoSafe gebruiken door het bedrijf beheerde mobiele apparaten om de beveiliging te waarborgen bij het werken met bedrijfsmiddelen, inclusief een antivirusprogramma. Dit wordt afgedwongen door software voor mobiel apparaatbeheer en kan niet worden gedeactiveerd door gebruikers.

Freelancers die bij SoSafe komen, worden afhankelijk van hun werkverantwoordelijkheden en toegangsbehoeften, uitgerust met mobiele apparaten om hetzelfde beveiligingsniveau te garanderen bij derden. Onder deze apparatuur valt bijvoorbeeld het verstrekken van virtuele machines of volledig beheerde mobiele apparaten.

Alle medewerkers worden getraind in goed gebruik van mobiele apparaten.

Beveiliging van dagelijkse processen en activiteiten

Log management

→ **Vereiste loggingactiviteiten**
Alle hosts en netwerkapparatuur genereren beveiligingslogs voor alle systeemcomponenten.

Alle hosts en netwerkapparatuur geven waarschuwingen bij mislukte beveiligingslogverwerking, zoals software-/hardwarefouten, storingen in de logvastlegmechanismen en het bereiken of overschrijden van de opslagcapaciteit van logs. Alle waarschuwingen moeten zo dicht mogelijk bij realtime worden afgegeven.

→ **Gecentraliseerd loggen**
Beveiligingsgebeurtenissen worden in realtime of zo snel als technologisch mogelijk is, overgedragen naar een beheerde loggingservice. De integriteit van logs voor geconsolideerde log infrastructuur wordt bewaard, bijvoorbeeld door logs op te slaan in alleen-lezenmodus.

→ **Vereiste monitoringactiviteiten**
Processen worden ontwikkeld en geïmplementeerd om logs voor alle systemen te controleren op anomalieën of verdachte activiteiten, zoals bij ons SIEM-systeem. Beveiligingsbaselines worden ontwikkeld en geautomatiseerde monitoringtools worden gebruikt om waarschuwingen te genereren wanneer uitzonderingen worden gedetecteerd.

→ **Geautoriseerd personeel**
Logs worden beveiligd door de toegang te beperken tot personen die toegang nodig hebben om hun werk uit te voeren en bestanden te beschermen tegen ongeautoriseerde wijzigingen volgens het 'need-to-know'-principe. Toegang tot logbeheersystemen wordt geregistreerd.

→ **Compliance**
Gegevens worden veilig gelogd, waarbij rekening wordt gehouden met de vereisten voor logretentie, bedrijfseisen en wettelijke voorschriften (bijv. AVG, Bundesdatenschutzgesetz).

Elk log met persoonlijk identificeerbare informatie moet worden goedgekeurd door onze Functionaris voor Gegevensbescherming (FG).

→ **Retentie**
Elektronische logs die worden gegenereerd door de monitoring zoals beschreven in dit document, worden gedurende minimaal 90 dagen bewaard en zijn direct beschikbaar.

Continuïteit van bedrijfsvoering en rampenherstelmanagement

We hebben een plan voor het beheer van bedrijfscontinuïteit. Dit wordt beschreven in een beleid voor het beheer van bedrijfscontinuïteit en is gebaseerd op ISO 22301:2019 voor het beheer van bedrijfscontinuïteit.

Back-up management

We hanteren een uitgebreid back-up plan voor al onze activa en hebben een back-up beleid met vereisten voor elk daarvan.

We hebben specifieke vereisten geïmplementeerd voor onze databases met klantgegevens.

→ **Planning**
De database wordt elke nacht volledig geback-upt en vervolgens continu geback-upt via streaming WAL (write-ahead logging).

→ **Hersteltijddoelstellingen**
Als volledig herstel nodig is (volledige database crash), hebben we tussen de 1 uur en 1 uur en 30 minuten nodig, afhankelijk van de omvang van de WAL. In geval van gedeeltelijk gegevensverlies kunnen we binnen 1 uur een volledig werkende replica van de productie opzetten en de benodigde gegevens herstellen.

Data veilig houden

Datacenters

Zowel de SoSafe data als gegevens van klanten worden gehost in AWS cloud, dat een zeer hoog fysiek beveiligingsniveau biedt. Er is geen grote bedreiging voor onze fysieke beveiliging, aangezien we een cloudgeoriënteerd bedrijf zijn. Bovendien biedt het datacenter meerdere beveiligingsmaatregelen om klantgegevens te beschermen volgens de hoogste beveiligingsnormen.

Data-encryptie

Alle klantgegevens in onze producten worden versleuteld tijdens de overdracht over openbare netwerken met minimaal TLS 1.2 om ze te beschermen tegen ongeautoriseerde openbaarmaking of wijziging. Onze implementatie van TLS dwingt het gebruik af van sterke versleutelingsmethoden en sleutellengtes, indien ondersteunt door de browser. Al onze systemen en gegevensstations die klantinformatie bevatten, maken in rust gebruik van volledige schijf-versleuteling met industriestandaard AES en volgen de richtlijnen van het BSI (Duitse Federale Bureau voor Informatiebeveiliging) bij het selecteren van cryptografische procedures, algoritmen en sleutellengtes.

Key management

SoSafe maakt gebruik van geavanceerde technologieën voor het veilig genereren, opslaan, archiveren, ophalen, distribueren, intrekken en verwijderen van de sleutels volgens de aanbevelingen van het National Institute of Standards and Technology (NIST).

Privésleutels worden opgeslagen in een wachtwoordmanager, wat ongeautoriseerde toegang onmogelijk maakt.

Het controleren van toegang tot klantgegevens

We hebben geen voorzieningen nodig voor speciale categorieën van persoonsgegevens, hoewel we alle klantgegevens als even gevoelig behandelen en strikte controles hebben geïmplementeerd om toezicht te houden op deze gegevens. Binnen SoSafe hebben alleen geautoriseerde SoSafe medewerkers toegang tot klantgegevens die binnen onze systemen zijn opgeslagen.
Alle toegang is beperkt tot bevoorrechte groepen, tenzij het verzoek wordt ingediend en beoordeeld op geldigheid, zoals verzoeken van klanten om toegang tot de gegevens, waarbij extra authenticatie is vereist middels 2FA.
Ongeautoriseerde of ongepaste toegang tot klantgegevens wordt behandeld als een beveiligingsincident en wordt beheerd via ons incidentbeheerproces. Dit proces omvat instructies om getroffen klanten op de hoogte te stellen als er een schending van het beleid wordt waargenomen.

Retentie en verwijdering van gegevens

→ **Klantgegevens**
Alleen klantstamgegevens (indien ze kwalificeren als persoonsgegevens) worden gedurende 10 jaar bewaard volgens §§ 147 AO, 257 HGB.

Archivering van de klantgegevens vindt plaats drie maanden na het verlopen van de licenties (om de gegevenskwaliteit te waarborgen voor eventuele latere licenties). Deze periode kan worden verlengd of verkort op verzoek van de klant.

Er wordt 4 weken vóór archivering een herinnering gestuurd naar de contactpersoon van de klant om de rapporten/certificaten te downloaden.

SoSafe houdt een bewijs van juiste vernietiging bij, volgens de ISO27001-standaard voor het verwijderen en afvoeren van gegevens, waarbij wordt vermeld dat alle opslagmedia worden geverifieerd om ervoor te zorgen dat alle gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig overschreven voordat ze worden verwijderd of hergebruikt.

Tijdens het verwijderen van de klantgegevens uit de SoSafe Management Software wordt een verwijderingsrapport gegenereerd dat de tijd en omvang van de verwijdering documenteert. Dit verwijderingsrapport wordt bewaard en op verzoek aan de klant getoond.

→ **Gegevens van de werknemers van de klant**
Het verwijderen van individuele gegevens of alle gegevens van werknemers van een klant is op elk moment handmatig mogelijk via het bedieningspaneel.

De toegang van gebruikers tot onze e-learning wordt gedeactiveerd aan het einde van de licentieperiode.

Persoonsgegevens van deelnemers aan een phishing simulatie of een e-learning campagne in de gebruikersdatabase, worden automatisch verwijderd wanneer de klantgegevens worden gearchiveerd (drie maanden na het verlopen van de licentie).

Tot 28 dagen na verwijdering kunnen de gegevens indien nodig nog worden gereconstrueerd uit back-ups.

→ **Actieve directory**
Als gebruikers in de Active Directory (AD) worden gedeactiveerd door de klant of het recht om de SoSafe E-Learning-applicatie te gebruiken verliezen, worden ze ook gedeactiveerd op het SoSafe-platform, kunnen ze niet meer inloggen en maken ze geen deel meer uit van de phishing campagnes.

Als gebruikers binnen 30 dagen opnieuw worden geactiveerd in de AD of het recht krijgen om de SoSafe E-Learning-applicatie te gebruiken, worden ze gereactiveerd en kunnen ze doorgaan met hun laatste status.

Na 30 dagen worden gedeactiveerde gebruikers verwijderd, inclusief voortgangsgegevens. Als de gebruikers dan opnieuw worden geactiveerd in de AD, worden er nieuwe gebruikers aangemaakt op het SoSafe-platform, die geen toegang meer hebben tot hun oude gegevens.

Beveiligen van onze mensen

Security awareness training

We zorgen ervoor dat alle medewerkers van SoSafe tijdens het onboardingsproces en vervolgens op doorlopende basis een training voor bewustwording van beveiliging volgen, zodat beveiliging een integraal onderdeel blijft van hun standaard denkwijze. De training wordt bekrachtigd door voortdurende phishing simulatie aanvallen waaraan onze medewerkers worden blootgesteld om hen voor te bereiden op en bewust te maken van echte aanvallen.

Onderwerpen die worden behandeld in ons trainingsprogramma voor bewustwording van beveiliging zijn actuele dreigingen en oplichting, veilige werkpraktijken, potentieel riskant gedrag dat beveiligingsrisico's creëert, en nalevings- en regelgevingskwesties.

Security Champions Programma

Met ons Security Champions Programma werken we aan een veiligheidscultuur binnen SoSafe die het bewustzijn van cybersecurity vergroot en de ontwikkeling en productuitgaven op het gebied van beveiliging versnelt en verbetert.

Onze focus ligt voornamelijk op de afdelingen productontwikkeling en techniek, waar we beveiligingskampioenen hebben die het gat vullen tussen de afdeling Application Security en ervaringsteams, en ervoor zorgen dat onze beveiligingspoorten worden nageleefd en dat de beveiligingscontroles niet worden omzeild in de levenscyclus van de softwareontwikkeling.

Bescherming tegen beveiligings-dreigingen

Testen van de beveiliging

Beveiligingstesten zijn een belangrijk onderdeel van de ontwikkelingslevens-cyclus en zijn zowel in de implementatiefase als ook in de testfase van de Secure Development Life Cycle (SDLC) onderdeel van de aanpak.

Beveiligingstesten worden uitgevoerd met behulp van onze tools in de implementatiefase, en volgt een 'shift-left'-benadering om ervoor te zorgen dat ontwikkelaars veilige code schrijven. Bovendien worden alle open-source externe bibliotheken die in ons product worden gebruikt, voortdurend gemonitord.

In de testfase wordt het beveiligingstesten gegarandeerd door de Application Security Engineers, en ondergaan alle belangrijke functies een dynamische beveiligingstest.

Vulnerability management

→ **Scannen op kwetsbaarheden**
Ons platform wordt continu gemonitord door automatische kwetsbaarheidsscans uit te voeren en ontdekte kwetsbaarheden onmiddellijk te herstellen.

→ **Scannen van externe open-source bibliotheken**
De externe open-source bibliotheken die we gebruiken, worden voortdurend gescand door onze Software Composition Analysis en doorgegeven aan het juiste team voor patching. De bibliotheken worden gepatcht met inachtneming van de SLA's die zijn gedefinieerd op basis van de ernst van de kwetsbaarheden.

Melden van incidenten

→ **Testen van respons op beveiligingsincidenten**
Om adequaat te kunnen reageren op een echte aanval, is het noodzakelijk dat alle belanghebbenden van tevoren weten hoe ze moeten reageren en wat ze moeten doen. SoSafe voert regelmatig incident response simulaties uit om een goede aanpak van incidenten te ontwikkelen.