

SoSafe voldoet aan de normen en richtlijnen van cyberverzekeringen



Bij het aanvragen van cyberverzekeringen worden risicobeoordelingen uitgevoerd. Daarbij wordt gekeken naar de bescherming van gevoelige gegevens, het voorkomen van IT-bedrijfsonderbrekingen, het onderhoud en beheer van IT en meer. Ontdek hoe onze oplossing jou kan helpen bij het verkrijgen van cyberverzekeringen!

Belangrijke voorwaarden	SoSafe oplossing
CSAT (Cyber Security Awareness Training)	Een eenvoudig te implementeren en op gedragswetenschap gebaseerd doorlopend bewustzijnstrainingsprogramma met een blijvende impact.
Rapportage-eisen	Audit-klaar dashboard vereenvoudigt rapportage ten behoeve van je cyberverzekering, ISO 27001, IEC-27001, TISAX en meer.
ISO 27001 kader	De beoordelingsmethoden van verzekeraars zijn vaak in lijn met het ISO 27001 kader. Goed om te weten dat SoSafe op basis van ISO 27001 is ontworpen.
Wachtwoordmanagement	Onze 'wachtwoordbeveiliging'-modules zorgen voor het versneld aanleren van het gewenste veilige gedrag.
Gegevensbeveiliging & AVG	SoSafe is AVG-compliant en volgt een privacy-by-design aanpak.
Beveiligingscultuur – Jouw bescherming tegen bedrijfsonderbrekingen als gevolg van verstoring van de IT-infrastructuur	Medewerkers zijn je belangrijkste asset. Met SoSafe worden zij continu getraind om zichzelf te beschermen tegen cyberaanvallen.
Andere belangrijke eisen: regelmatige back-ups; frequente patching; bescherming tegen malware en antivirus aanwezig en up-to-date; firewall geïnstalleerd en correct geconfigureerd; multifactorauthenticatie	



Vraag na bij je verzekeraar

Afhankelijk van de grootte van je organisatie, kan CSAT een verplichte voorwaarde zijn voor een cyberverzekering.



In sommige gevallen verlaagt CSAT de kosten van cyberverzekeringen.

Heb je CSAT op korte termijn nodig?

Wij garanderen een implementatie binnen 20 dagen.

Demo aanvragen →

sosafe-awareness.com