

Vragenlijst voor Leveranciers

ISO/IEC 27001:2022 Conformiteit

Organisatie Context

- Heeft u gekeken naar de zaken zowel binnen als buiten uw organisatie die invloed hebben op de beveiliging van uw informatie, en dit opgeschreven in beleid? (Binnen: zoals het aantal en de kennis van uw medewerkers; Buiten: zoals de wetten die voor u gelden.)
- Hoe houdt u rekening met informatiebeveiliging bij het bereiken van de doelen van uw organisatie?

Leiderschap en Betrokkenheid

- Is uw management actief betrokken bij het opzetten en onderhouden van informatiebeveiliging?
- Heeft uw organisatie een goedgekeurd informatiebeveiligingsbeleid dat actief wordt gedeeld?
- Hoe zorgt het management ervoor dat medewerkers hun rol in informatiebeveiliging begrijpen? (Denk aan posters op de werkvloer, e-learning, gedragscode etc)

Risico's

- Hoe identificeert u risico's en kansen op het gebied van informatiebeveiliging? (Bijvoorbeeld risicoanalyses die periodiek worden gemaakt)
- Hoe beoordeelt en behandelt u beveiligingsrisico's?
- Welke maatregelen heeft u genomen om risico's te beheersen? Kunt u een voorbeeld geven?

Ondersteuning

- Heeft u genoeg middelen (personeel, technologie, budget) om informatiebeveiliging te borgen?
- Hoe zorgt u ervoor dat medewerkers op de hoogte zijn van hun rol in informatiebeveiliging?
- Welke documentatie gebruikt u voor informatiebeveiliging en hoe houdt u deze up-to-date?

Operationele Processen

- Hoe zorgt u ervoor dat beveiligingsmaatregelen goed worden uitgevoerd in de dagelijkse werkzaamheden?
- Welke maatregelen heeft u genomen om de toegang tot gevoelige informatie te beperken?
- Hoe beveiligt u gegevens, zowel tijdens transport als in rust (bijvoorbeeld door versleuteling)?

Evaluatie van Prestaties

- Voert u regelmatig interne audits uit om de effectiviteit van de informatiebeveiliging te controleren? Hoe vaak?
- Wat doet u met de resultaten van deze audits?
- Heeft u prestatie-indicatoren (KPI's) om de effectiviteit van de informatiebeveiliging te meten?

Verbetering

- Hoe identificeert u verbeterpunten voor informatiebeveiliging?
- Kunt u een voorbeeld geven van een verbetering die u heeft doorgevoerd na een beveiligingsincident of audit?
- Hoe zorgt u ervoor dat beveiligingsincidenten goed worden onderzocht en er passende maatregelen worden genomen?

Risicobeheer

- Hoe past u informatieclassificatie toe om gevoelige informatie te identificeren?
- Welke methoden gebruikt u om risico's in de informatiebeveiliging te beoordelen en te beheren?
- Hoe zorgt u ervoor dat risico's adequaat worden behandeld (bijvoorbeeld door technische of organisatorische maatregelen)?

Beheersmaatregelen (Annex A)

- Welke maatregelen heeft u genomen om ongevoegde toegang tot gevoelige informatie te voorkomen (bijvoorbeeld toegangscontrole)?
- Gebruikt u versleuteling om gevoelige informatie te beschermen? Zo ja, hoe implementeert u dit?
- Wat is uw procedure voor het melden, onderzoeken en oplossen van beveiligingsincidenten?
- Hoe zorgt u ervoor dat uw organisatie blijft draaien tijdens en na een beveiligingsincident (bijvoorbeeld met een continuïteitsplan)?