NIS2 afspraken voor kleine opdrachtnemers minder dan 50 werknemers

Doel: aantonen dat jouw organisatie voldoet aan basis cybersecurity-eisen volgends de NIS2-wetgeving.

1. Beveiligingsmaatregelen

- Antivirus/anti-malware software geïnstalleerd en up to date
- Firewalls en netwerkbeveiliging geconfigureerd
- Regelmatige software- en systeemupdates (patchmanagement)
- Encryptie van gevoelige data waar nodig

2. Risicobeheer

- Cybersecurityrisico's in kaart gebracht
- Maatregelen genomen om geïdentificeerde risico's te mitigeren
- Eventuele leveranciers- of ketenrisico's beoordeeld

3. Incidentmanagement

- Procedure voor het melden van beveiligingsincidenten opgesteld
- Incidenten kunnen binnen afgesproken termijn worden gemeld aan opdrachtgever
- Basisregistratie van incidenten bijgehouden

4. Toegangsbeheer & authenticatie

- Sterke wachtwoorden ingesteld en periodiek vernieuwd
- Multi-factor authentication (MFA) waar mogelijk toegepast
- Toegangsrechten afgestemd op functie ("need-to-know")

5. Continuïteit & back-up

- Regelmatige back-ups van belangrijke data
- Back-ups getest en herstelprocedures bekend
- Noodplan beschikbaar voor kritieke processen

6. Security awareness

- Personeel getraind in basis cyberveiligheid (phishing, wachtwoorden, veilig gebruik systemen)
- Periodieke bewustwordingssessies gepland

7. Audit & rapportage

- Periodieke interne controles of audits uitgevoerd
- Beveiligingsmaatregelen gedocumenteerd en rapporteerbaar naar opdrachtgever

- Eventuele verbeteracties vastgelegd

8. Contractuele compliance

- Cybersecurity-eisen uit contract met opdrachtgever geïnventariseerd
- Procedures en maatregelen afgestemd op eisen van opdrachtgever
- Documentatie beschikbaar om compliance aan te tonen