

Checklist Cyberbeveiligingswet (NIS2)



Voor de directie · Bijgewerkt op 16 oktober 2026 · Dit is geen juridisch advies

Loop deze vragen samen door. Elk vakje dat u niet kunt aankruisen, is een actiepunt.

1. Valt u eronder?

- ☐ Wij zijn zelf actief in een sector uit bijlage 1 of 2 van de wet.
- ☐ Wij hebben 50 fte of meer, of een jaaromzet én balanstotaal van elk meer dan € 10 miljoen (partner- en verbonden ondernemingen tellen mee).
- ☐ Wij hebben de NIS2-zelfevaluatie van de RDI gedaan en weten of wij essentieel of belangrijk zijn.
- ☐ Vallen wij er niet onder: wij weten welke klanten er wel onder vallen en welke eisen zij aan ons kunnen stellen.

2. Registratie

- ☐ Onze organisatie staat in het entiteitenregister op mijn.ncsc.nl.
- ☐ Er is eHerkenning op niveau EH2+ met de juiste machtiging.
- ☐ Contactpersoon en netwerkgegevens (IP-adressen, domeinnamen) zijn actueel. Wijzigingen geven wij binnen twee weken door.

3. Zorgplicht: de tien onderwerpen

- ☐ Risicoanalyse en beveiligingsbeleid
- ☐ Incidentbehandeling
- ☐ Bedrijfscontinuïteit: back-up, herstel en crisisbeheer
- ☐ Beveiliging van de toeleveringsketen
- ☐ Veilige aanschaf, ontwikkeling en onderhoud, met omgaan met kwetsbaarheden
- ☐ Toetsen of de maatregelen werken
- ☐ Basishygiëne en training voor medewerkers
- ☐ Cryptografie en versleuteling
- ☐ Personeelsbeveiliging, toegangsbeleid en beheer van bedrijfsmiddelen
- ☐ Multifactorauthenticatie en beveiligde communicatie

4. Meldplicht

- ☐ Wij zien een aanval op tijd, ook buiten kantoortijd.
- ☐ Er is een incidentprocedure: wie beslist of een incident significant is, en wie meldt.
- ☐ Wij kunnen binnen 24 uur waarschuwen, binnen 72 uur melden en binnen een maand een eindverslag sturen.

5. Bestuur

- ☐ Het bestuur heeft de maatregelen goedgekeurd.
- ☐ Bestuurders hebben een training gevolgd en hebben het certificaat.
- ☐ Het bestuur krijgt regelmatig een rapportage over cyberrisico's en de voortgang.