ICTRECHT

FACTSHEET

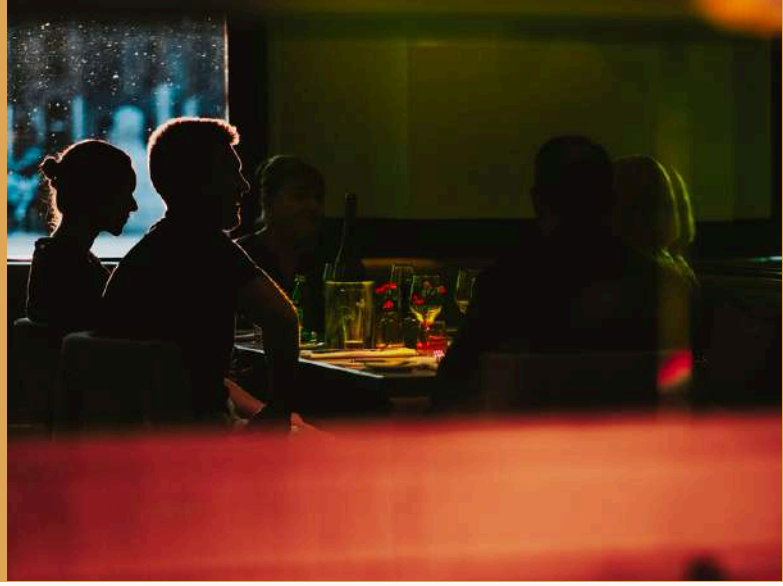
NIS2 / Cyberbeveiligingswet

Weet in 1 minuut alles over de nieuwe regels

SCOPE

Wat is de cyberbeveiligingswet (Cbw)?

De Cbw is de Nederlandse implementatie van de Europese NIS2-richtlijn. De wet heeft als doel de digitale weerbaarheid van Nederland te versterken door eisen te stellen aan de beveiliging van netwerk- en informatiesystemen.



Doelstellingen

Richt zich op 4 pijlers:

Risicobeheer
Beheersen van risico's voor netwerk- en informatiesystemen

Preventie
Voorkomen van incidenten

Schadebeperking
Beperken van gevolgen van incidenten

Informatiedeling
Verkrijgen en verstrekken van informatie over incidenten, dreigingen en kwetsbaarheden

Sectoren

De Cbw is van toepassing op organisaties in de volgende sectoren

Zeer kritieke sectoren (Bijlage 1 NIS2)

- Energie
- Vervoer
- Bankwezen
- Infrastructuur voor de financiële markt
- Gezondheidszorg
- Drinkwater
- Afvalwater
- Digitale infrastructuur
- Beheer van ICT-diensten (business-to-business)
- Overheid
- Ruimtevaart
- Hoger Onderwijs*

Andere kritieke sectoren (Bijlage 2 NIS2)

- Post- en Koeriersdiensten
- Afvalstoffenbeheer
- Vervaardiging, productie en distributie van chemische stoffen
- Productie, verwerking en distributie van levensmiddelen
- Vervaardiging
- Digitale aanbieders
- Onderzoek

*Het Hoger Onderwijs is door de Minister van Onderwijs aangewezen als sector om te voldoen aan de Cbw.

Voor wie?

De NIS2/Cbw is van toepassing op organisaties die:

1. Actief zijn in één van de genoemde sectoren, én;
2. voldoen aan de omvangscriteria:

Criterium	Middelgrote organisatie	Grote organisatie
Werknemers (FTE)	50-249	>250
Jaaromzet	€10-50 miljoen	>€50 miljoen
Balanstotaal	€10-43 miljoen	>€43 miljoen

Let op:
Voor bepaalde sectoren gelden de omvangscriteria niet, zoals voor:

- Verleners van vertrouwensdiensten
- Aanbieders van openbare elektronische communicatie-netwerken
- TLD-naamregisters en DNS-dienstverleners
- Overheidsinstanties
- Entiteiten die door de overheid zijn aangewezen

Uitgezonderd: De wet is niet van toepassing op:

- Kleine organisaties: < 50 FTE en een jaaromzet of balanstotaal <€10 miljoen
- Entiteiten die uitsluitend activiteiten uitvoeren op het gebied van:
  - Nationale veiligheid
  - Openbare veiligheid
  - Defensie
  - Rechtshandhaving

Essentiële of belangrijke entiteit

De Cbw onderscheidt 2 categoriën entiteiten:

Type entiteit	Kenmerken
Essentiële entiteit	Grote organisaties in zeer kritieke sectoren
Belangrijke entiteit	Middelgrote organisaties in zeer kritieke sectoren én middelgrote/grote organisaties in andere kritieke sectoren

Waarom is dit onderscheid belangrijk?

Aspect	Essentiële entiteit	Belangrijke entiteit
Toezicht	Proactief (vooraf)	Reactief (achteraf)
Sancties	Hoger sanctieregime	Lager sanctieregime

Zelf bepalen

Organisaties moeten zelf beoordelen of zij onder de wet vallen en in welke categorie zij thuishoren.
Dit vorm de basis voor de registratieplicht.

Verplichtingen

Registratieplicht

Entiteiten moeten zicht registreren bij de toezichthouder via mijn.ncsc.nl. Hierbij verstrekken zij minimaal de volgende gegevens:

- Naam van de entiteit
- Adres en contactgegevens (inclusief e-mailadress en telefoonnummers)
- Relevante sector en subsector
- Lidstaten waar de entiteit actief is
- IP-adressen

Bijwerken: Wijzingen moet binnen **twee weken** worden doorgegeven

Governance

Het bestuur van entiteiten is verplicht:

Verplichting	Toelichting
Goedkeuren	Maatregelen voor risicobeheer moeten door het bestuur worden goedgekeurd
Toezicht houden	Het bestuur houdt toezicht op de uitvoering van de maatregelen
Opleiding volgen	Bestuursleden moeten voldoende kennis en vaardigheden opdoen om risico's te identificeren en te beoordelen. Binnen 2 jaar na ingang van de wet en certificaat van deelname
Aansprakelijkheid	Bestuursleden kunnen aansprakelijk worden gesteld bij niet-naleving

Opleiding medewerkers:
Het bestuur moet ervoor zorgen dat ook medewerkers regelmatig cyberbeveiligingstraining krijgen. Bekijk hier ons overzicht van security-trainingen en opleidingen.

Meldplicht

Waneer melden? Bij een significant incident moet de entiteit dit melden bij het CSIRT en de toezichthouder (via mijn.ncsc.nl)

Wat is een significant incident? Een incident is significant als het:

- Ernstige operationele verstoring van diensten of financiële verliezen veroorzaakt (of kan veroorzaken)
- Andere natuurlijke of rechtspersonen aanzienlijke materiële of immateriële schade toebrengt (of kan toebrengen)

Controleer de ministeriële regeling voor de desbetreffende sector voor de drempelwaardes om te bepalen wanneer een significant incident zich voordoet.

Meldtermijnen

Fase	Termijn	Inhoud
Vroegtijdigewaarschuwing	Binnen 24 uur	Eerste melding: vermoedelijke oorzaak, grensoverschrijdend effect, mogelijk opzet
Incidentmelding	Binnen 72 uur	Eerste beoordeling: ernst, impact, indicatoren van compromitteren
Eindverslag*	Binnen 1 maand	Gedetailleerde beschrijving, oorzaak, genomen maatregelen, grensoverschrijdende impact

***Bij voortdurend incident:**
In plaats van een eindverslag een voortgangsverslag na 1 maand, en het eindverslag binnen 1 maand na afhandeling.

Zorgplicht

Kernverplichting - Entiteiten moeten **passende en evenredige technische, operationele en organisatorische maatregelen** nemen om risico's te beheren.

Verplichte maatregelen (minimaal)

Maatregel*

- Beleid inzake risicoanalyse en beveiliging van informatiesystemen
- Incidentenbehandeling
- Bedrijfscontinuïteit, back-upbeheer, noodvoorzieningenplannen en crisisbeheer
- Beveiliging bij verwerven, ontwikkelen en onderhouden van systemen (incl. kwetsbaar-heidsbeheer)
- Beleid en procedures om effectiviteit van maatregelen te beoordelen
- Basispraktijken op het gebied van cyberhygiëne en opleiding
- Beleid inzake het gebruik van cryptografie en encryptie
- Beveiligingsaspectten m.b.t. personeel, toegangsbeleid, en beheer van assets
- Wanneer gepast, multi-factor authenticatie, beveiligde communicatie en noodcommunicatie-systemen

*Controleer de sector specifieke ministeriële regeling om te controleren hoe je moet voldoen aan de zorgplicht. In sommige gevallen voldoe je aan de zorgplicht wanneer je voldoet aan: ISO 27001:2022, NEN7510:2024 of BIO 2.0.

Afwegingsfactoren - Bij het bepalen van de juiste maatregelen houdt rekening met:

- De stand van de techniek
- Kosten van de uitvoering
- Europese en internationale normen
- Mate van blootstelling aan risico's
- Omvang van de entiteit
- Kans op incidenten en de ernst ervan (inclusief maatschappelijke en economische gevolgen)

Sancties en tijdslijn

Sanctieregime

De toezichthouder kan verschillende sancties opleggen bij niet-naleving:

Sanctie	Toelichting
Waarschuwing	Bij minder ernstige overtredingen
Bindende aanwijzingen	Verplichte instructies om naleving te bereiken
Last onder dwangsom	Dwangsom tot naleving is bereikt
Bestuurlijke boete	Financiële sanctie

Maximale boetes

Type entiteit	Maximale boete
Essentiële entiteit	€10 miljoen of 2% van de wereldwijde jaaromzet (hoogste van de twee)
Belangrijke entiteit	€7 miljoen of 1,4% van de wereldwijde jaaromzet (hoogste van de twee)

Persoonlijke aansprakelijkheid

Bestuursleden kunnen persoonlijk aansprakelijk worden gesteld voor het niet naleven van de verplichtingen uit de wet

Aanvullende maatregelen voor essentiële entiteiten

Bij ernstige niet-naleving kunnen aanvullende maatregelen worden opgelegd:

- Tijdelijk verbod op uitoefening leidinggevende functies
- Tijdelijke opschorting van certificaten of vergunningen

Vanaf wanneer?

Datum	Gebeurtenis
16 januari 2023	NIS2-richtlijn in werking getreden
17 oktober 2024	NIS2-richtlijn moet omgezet zijn naar nationale wetgeving. Nederlandse wet heeft vertraging
Juni 2025	Wetsvoorstel ingediend bij de Tweede Kamer
15 april 2026	Tweede Kamer stemt in met de Cyberbeveiligingswet
Q2 2026 (prognose)	Behandeling in de Eerste Kamer en beoogde inwerkingtreding

Aanbeloven acties:

1. Bepaal of jouw organisatie onder de Cbw valt en welke classificatie jouw organisatie krijgt
2. Voer een GAP-analyse uit
3. Stel een implementatieplan op
4. Begin met trainen van bestuur en medewerkers
5. Bereid registratie- en meldprocedures voor

Dit zijn acties waar ICTRecht mee kan helpen. Ga voor meer informatie naar:
https://www.ictrecht.nl/security-compliance

Wil je meer weten over de NIS2?

Bezoek onze website voor het laatste nieuws, onze diensten en trainingen.

Vragen?

www.ictrecht.nl/nis2
020 - 663 1941