

Checklist Dutch Cybersecurity Act (NIS2)



For the board · Updated on 16 October 2026 · This is not legal advice

Go through these questions together. Every box you cannot tick is an action point.

1. Does it apply to you?

- ☐ We are active ourselves in a sector from Annex 1 or 2 of the act.
- ☐ We have 50 FTE or more, or an annual turnover and balance sheet total of more than € 10 million each (partner and linked enterprises count).
- ☐ We have taken the NIS2 self-assessment of the RDI and know whether we are essential or important.
- ☐ If we are not covered: we know which customers are, and what requirements they can set for us.

2. Registration

- ☐ Our organisation is in the entity register at mijn.ncsc.nl.
- ☐ We have eHerkenning at level EH2+ with the right authorisation.
- ☐ Contact person and network details (IP addresses, domain names) are up to date. We report changes within two weeks.

3. Duty of care: the ten topics

- ☐ Risk analysis and security policy
- ☐ Incident handling
- ☐ Business continuity: backup, recovery and crisis management
- ☐ Supply chain security
- ☐ Secure acquisition, development and maintenance, with vulnerability handling
- ☐ Assessing whether the measures work
- ☐ Basic cyber hygiene and training for employees
- ☐ Cryptography and encryption
- ☐ HR security, access control and asset management
- ☐ Multi-factor authentication and secured communications

4. Reporting obligation

- ☐ We see an attack in time, also outside office hours.
- ☐ There is an incident procedure: who decides whether an incident is significant, and who reports.
- ☐ We can warn within 24 hours, notify within 72 hours and send a final report within one month.

5. Board

- ☐ The board has approved the measures.
- ☐ Board members have taken a training and hold the certificate.
- ☐ The board regularly receives a report on cyber risks and progress.