**Dit is een voorbeeld.** Het bedrijf op deze pagina is verzonnen. Zo ziet de Ketenpas eruit die u naar uw klant stuurt in plaats van zijn vragenlijst in te vullen; uw eigen pas krijgt uw naam, scores en huisstijl.

---

SECURITY PASPOORT

# Voorbeeld Installatietechniek B.V.

Elektrotechniek en klimaatinstallaties voor zorg en industrie




Goed

Deze organisatie heeft haar informatiebeveiliging beoordeeld langs de tien maatregelen uit artikel 21 van de NIS2-richtlijn, de basis van de Nederlandse Cyberbeveiligingswet.

**27 van de 39 maatregelen zijn op orde.**

| Beoordeeld op | Geldig tot | Grondslag |
|---|---|---|
| 14 oktober 2026 | 14 oktober 2027 | NIS2 artikel 21, 39 punten |

## Maatregelen per onderdeel

Hieronder staat per onderdeel wat deze organisatie heeft ingericht.

### Risicoanalyse en beveiligingsbeleid — 90%

- ✓ Is er een informatiebeveiligingsbeleid dat de directie heeft vastgesteld onderbouwd A.5.1
- ✓ Heeft u in de afgelopen twaalf maanden een risicoanalyse gedaan 6.1.2
- ✓ Is vastgelegd wie binnen uw organisatie eindverantwoordelijk is voor cybersecurity A.5.2

## Incidentafhandeling 90%

- ✓ Is er een vastgelegde procedure voor wat u doet bij een cyberincident onderbouwd A.5.24 A.5.26
- ✓ Weten uw medewerkers bij wie ze een verdachte melding of incident moeten melden A.6.8
- ✓ Kunt u een ernstig incident binnen 24 uur melden aan uw klanten en het CSIRT A.5.5 A.5.26

## Bedrijfscontinuïteit en back-ups 91%

- ✓ Worden er automatisch back-ups gemaakt van al uw bedrijfskritische gegevens onderbouwd A.8.13
- ✓ Staat minstens één back-up buiten bereik van uw netwerk A.8.13
- ✓ Heeft u het afgelopen jaar getest of terugzetten uit back-up echt werkt onderbouwd A.8.13 A.5.30

## Beveiliging van de toeleveringsketen 67%

- ✓ Heeft u een overzicht van uw ICT-leveranciers en welke toegang zij hebben A.5.19 A.5.21
- ✓ Staan er beveiligingsafspraken in de contracten met uw belangrijkste leveranciers A.5.20

## Aanschaf, ontwikkeling en onderhoud 90%

- ✓ Worden updates en beveiligingspatches structureel en tijdig geïnstalleerd onderbouwd A.8.8
- ✓ Heeft u zicht op welke apparaten en software er in uw netwerk staan A.5.9
- ✓ Draait u nog op software of apparatuur die geen updates meer krijgt A.8.8

## Toetsen van effectiviteit 60%

- ✓ Toetst u periodiek of uw beveiligingsmaatregelen echt werken A.5.36

## Cyberhygiëne en training

94%

- ✓ Krijgen alle medewerkers minstens jaarlijks bewustwordingstraining onderbouwd A.6.3
- ✓ Zijn er duidelijke regels over wachtwoorden, thuiswerken en privégebruik A.5.10 A.6.7
- ✓ Volgt de directie zelf ook cybersecuritytraining A.6.3 A.5.4

## Cryptografie en encryptie

100%

- ✓ Zijn laptops en mobiele apparaten versleuteld onderbouwd A.8.1 A.8.24
- ✓ Wordt gegevensuitwisseling versleuteld verzonden A.5.14 A.8.24
- ✓ Zijn uw back-ups versleuteld opgeslagen A.8.13 A.8.24

## Personeel, toegangsbeheer en bedrijfsmiddelen

78%

- ✓ Krijgen medewerkers alleen toegang tot wat ze voor hun werk nodig hebben A.5.15 A.5.18
- ✓ Wordt toegang direct ingetrokken als iemand uit dienst gaat onderbouwd A.5.18 A.6.5
- ✓ Heeft u een overzicht van bedrijfsmiddelen en wie ze in gebruik heeft A.5.9 A.5.11

## Meervoudige authenticatie en veilige communicatie

91%

- ✓ Is meervoudige authenticatie verplicht op e-mail en alle systemen die vanaf internet bereikbaar zijn onderbouwd A.8.5
- ✓ Gebruiken beheerders MFA én aparte beheeraccounts A.8.2 A.8.5
- ✓ Is toegang op afstand beveiligd met meervoudige authenticatie A.8.5 A.6.7

## Over dit paspoort

Dit overzicht is gebaseerd op zelfrapportage door de organisatie zelf. Het is geen certificering en geen audit, en Ketenpas heeft de antwoorden niet geverifieerd. Wilt u zekerheid op een specifiek punt, vraag dan om onderliggend bewijs.

Bij 9 van de 27 bevestigde maatregelen heeft deze organisatie onderliggend bewijs vastgelegd, zoals beleid of een testrapport. Die stukken staan bewust niet op deze pagina; vraag ze op bij de organisatie zelf.

Openstaande punten worden hier niet getoond. Een deelbare pagina die precies benoemt welke beveiliging ontbreekt, zou een aanvaller de weg wijzen. De score en het aantal van 39 maatregelen geven aan hoeveel er nog te doen is.

De nummers bij de maatregelen verwijzen naar de corresponderende beheersmaatregelen uit ISO 27001:2022; A. wijst naar bijlage A, nummers zonder A. naar de hoofdtekst van de norm. De verwijzing toont aansluiting op de norm en is geen certificering.

---

Vragen over dit paspoort? **Voorbeeld Installatietechniek B.V., ICT**

---