



NIS2 Leveranciersverklaring

Organisatie	GP Groot bv
KvK-nummer	37041433
Adres	Vennewatersweg 2b, 1852 PT Heiloo
Contactpersoon security	Robert Quant, ICT Manager
E-mail security	securityofficer@gpgroot.nl
Versie / datum	V2.0 01-07-2026

1. Doel en scope

Deze verklaring beschrijft hoe GP Groot passende technische en organisatorische maatregelen heeft getroffen om informatiebeveiligingsrisico's te beheersen in lijn met de principes van de NIS2-richtlijn. De verklaring is specifiek opgesteld voor onze rol als leverancier binnen de ketens waarbinnen de GP Groot bedrijven actief zijn.

2. Onze rol in de keten

GP Groot levert producten en/of diensten die voor klanten onderdeel kunnen zijn van operationeel kritieke processen. Wij erkennen dat verstoringen in onze dienstverlening impact kunnen hebben op continuïteit, veiligheid, logistiek en operationele betrouwbaarheid bij onze klanten.

3. Uitgangspunten voor informatiebeveiliging

Onze maatregelen zijn risico gebaseerd ingericht en sluiten aan op erkende beveiligingskaders zoals ISO 27001, NIST Cybersecurity Framework en CIS Controls. De exacte invulling kan per dienst, locatie, applicatie of klantafpraak verschillen.

4. Overzicht beveiligingsmaatregelen

Domein	Maatregel
Governance	Informatiebeveiligingsbeleid, rollen en verantwoordelijkheden belegd.
Toegangsbeheer	MFA op kritieke systemen, rolgebaseerde rechten en periodieke accountreviews.
Netwerk & systemen	Segmentatie, endpointbeveiliging, logging en patchmanagement.
Incidentmanagement	Procedure voor detectie, beoordeling, escalatie en klantcommunicatie.
Continuïteit	Back-up, herstelafspraken, noodprocedures en hersteltests waar relevant.
Leveranciersbeheer	Security-eisen voor kritieke leveranciers en periodieke beoordeling.
Awareness	Bewustwordingstraining, phishingpreventie



NIS2 Leveranciersverklaring

5. Risicomanagement

Wij voeren periodiek een risicobeoordeling uit op kritieke processen, systemen en leveranciers. Hierbij is specifiek aandacht voor ketenafhankelijkheden, operationele continuïteit, bescherming van klantinformatie, en integraties tussen IT- en operationele processen.

6. Incidentmelding en communicatie

Bij een beveiligingsincident dat impact kan hebben op de dienstverlening aan klanten, wordt het incident beoordeeld op ernst, omvang, impact en meldplicht. Indien relevant informeren wij betrokken klanten via het vastgestelde contactpunt.

7. Samenwerking met security partner

GP Groot pakt de verdere uitwerking, toetsing en verbetering van deze beveiligingsmaatregelen samen op met een gespecialiseerde securitypartner. Deze securitypartner ondersteunt ons met specialistische kennis op het gebied van informatiebeveiliging, risicobeoordeling, monitoring en opvolging van verbeterpunten. Hiermee borgen wij dat onze aanpak niet alleen intern wordt vastgesteld, maar ook extern wordt getoetst.

8. Verklaring

GP Groot bv verklaart dat passende maatregelen zijn ingericht om informatiebeveiligingsrisico's en continuïteitsrisico's te beheersen binnen de scope van deze verklaring. Deze maatregelen zijn afgestemd op de aard van onze dienstverlening, de risico's in de keten en de verwachtingen vanuit klanten en wet- en regelgeving, waaronder de NIS2-richtlijn.

Deze verklaring is geen certificering en vervangt geen klantspecifieke audit of contractuele beveiligingsafspraken. Indien gewenst kunnen aanvullende afspraken, audits of vragenlijsten separaat worden overeengekomen.

9. Ondertekening

Naam	Ilse Oud
Functie	Financieel Directeur
Datum	01-07-2026
Plaats	Heiloo
Handtekening	I.Oud Digitaal ondertekend door I.Oud DN: cn=I.Oud, email=I.Oud@gpgroot.nl Datum: 2026.07.08 14:30:42 +02'00'