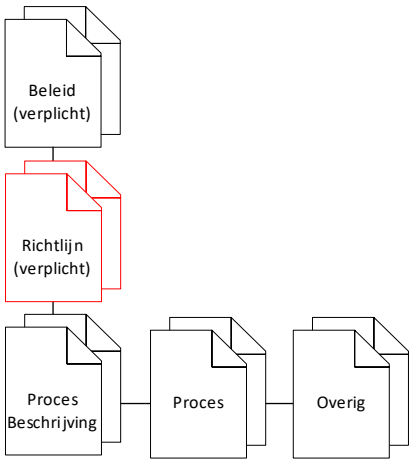
Provincie Noord-Brabant

Informatiebeveiliging
DOC-BB-01B
Richtlijn: Security Eisen PNB Leveranciers



Datum: 29-10-2025
Versie: 1.0
Auteur: Robin Toornstra
Eigenaar: Directie
Status: Final
Type: Richtlijn

LICENTIEBEHEER

Voor vragen of meer informatie kunt u contact opnemen met:

P.H.W. van den Boogaard
Chief Information Security Officer
Provincie Noord-Brabant
Brabantlaan 1
5216 TV 's-Hertogenbosch

Versiebeheer

Versie	Datum	Omschrijving reden nieuwe versie
0.1	25-05-2025	Initiële versie ter review
0.9	01-10-2025	Review commentaar verwerkt
1.0	29-10-20205	Inhoud in PNB template opgenomen

Verspreiding

Versie	Datum	Verspreiding
0.1	25-05-2025	CISO Office
0.9	01-10-2025	Final draft versie voor input inkooptraject Leerplatform
1.0	29-10-2025	PNB Projecten en Inkoop organisatie

Documentgegevens

Onderwerp	Omschrijving
Documentnaam:	DOC-BB-01[B] Richtlijn: Security Eisen PNB Leveranciers.docx
Aantal pagina's:	
Opsteller:	Robin Toornstra
Status:	Final
Classificatie:	Publiek

Verwijzingen

Verwijzing	Titel	Versie
NEN-ISO 27001	Information Security Management System (ISMS)	2024
NEN-ISO 27002	Information Security Controls; Cybersecurity & Privacy Bescherming	2022
NEN-ISO 31000	Risk Management Guidelines	2018
BIO	Baseline Informatiebeveiliging Overheid	2.0
NIS2-richtlijn	Directive (EU) 2022/2555	14 december 2022
Voorstel Cyberbeveiligingswet (Cbw) Nederland	Nederlandse omzetting van NIS2 in nationale wetgeving: omvat sectoren, meldplichten, risicobeheer e.d	Verwacht Q2 2026 (wetsvoorstel Q2 2025)

Acceptatie

Acceptatie en goedkeuring	Datum	Corsa verwijzing
-	-	-

Inhoud

1. Inleiding

1.1. Doelstelling

1.2. Reikwijdte

Deze richtlijn geldt voor alle medewerkers en derden personen die gebruik maken van de informatievoorziening van de Provincie Noord-Brabant. En is van toepassing op de gehele informatievoorziening waar de Provincie Noord-Brabant verantwoordelijk voor is en/of gebruik van maakt.

2. Termen, definities en afkortingen

In de onderstaande paragrafen worden de voor het document relevante termen, definities en afkortingen opgesomd.

2.1. Termen en definities

2.2. Gebruikte afkortingen

Afkorting	Beschrijving
IB	Informatiebeveiliging
NEN-ISO 27001	Internationale standaard voor informatiebeveiliging
BIO	Baseline Informatiebeveiliging Overheid
NIS2	Directive (EU) 2022/2555

3. Security Richtlijnen

3.1. Introductie

De Provincie Noord-Brabant (PNB) is NEN-ISO 27001 gecertificeerd en voldoet additioneel ook aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO is een verplicht normenkader opgelegd vanuit de Rijksoverheid en geldt voor overheidsinstanties binnen Nederland zoals bijvoorbeeld rijk, provincies, waterschappen en gemeenten. De Provincie Noord-Brabant moet daarnaast ook voldoen aan de Europese NIS2 richtlijn. Bovengenoemde wet-, regelgeving en normenkaders dienen gezien te worden als de pijlers van informatiebeveiliging binnen de provinciale organisatie. Daarnaast heeft PNB ook nog te maken met andere wetgevingen en normenkaders of uitvloeisels daarvan zoals bijvoorbeeld de Archiefwet, Wet Digitale Overheid en Forum Standaardisatie.

3.2. Gecertificeerde Dienstverlening

Informatiebeveiliging stopt niet bij de provinciale organisatie. Het maakt in de huidige tijd ook steeds meer deel uit van de bedrijfsvoering van dienstendienstverleners en ketenpartners van of voor PNB. Om deze reden stelt de PNB eisen aan de dienstverlener en de geleverde diensten die onderdeel uitmaken van de keten:

- Dienstverleners en hun onderaannemers zijn NEN-ISO27001 gecertificeerd (of gelijkwaardig) voor de scope van de aangeboden dienstverlening;

- De dienstverlener conformeert zich aan de Baseline Informatiebeveiliging Overheid (BIO) en afgeleide wetgeving en/of normenkaders over de volledige scope van geleverde dienstverlening;

- PNB behoudt zich het recht voor om een (externe) audit, op kosten van PNB, uit te laten voeren waarna eventueel geconstateerde afwijkingen in overleg met PNB binnen een overeengekomen periode ingevuld dienen te worden;

- De dienstverlener conformeert zich vanaf de publicatie in de Staatscourant aan de toekomstige NIS2 wetgeving en de daaruit voortvloeiende cyberbeveiligingswet (CBW) voor de scope van geleverde dienstverlening.

3.3. Managementsysteem voor Informatiebeveiliging (ISMS)

BIO: Leverancier implementeert en onderhoud een ISMS conform ISO27001, zoals vereist door BIO, om informatiebeveiligingsrisico's systematisch te beheren. Voert regelmatig risicobeoordelingen uit om risico's voor vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van gegevens en diensten te identificeren, evalueren en mitigeren. Houdt documentatie bij van beveiligingsbeleid, procedures en risicobehandelingsplannen, met waarborging van traceerbaarheid en controleerbaarheid.

NIS2 Aanvulling: Leverancier ontwikkelt een uitgebreid informatiebeveiligingsbeleid dat risicoanalyses, beveiligingsdoelstellingen en verantwoordelijkheden van het management expliciet definieert, zoals voorgeschreven in NIS2. Zorgt ervoor dat het management actief toezicht houdt op en getraind wordt in cyberbeveiligingsmaatregelen, met aansprakelijkheid bij niet-naleving (bijv. boetes of tijdelijke uitsluiting van managementfuncties).

Praktisch: Leverancier documenteert een risicobeheerraamwerk dat zowel digitale als fysieke bedreigingen omvat, zoals vereist door NIS2's 'all-hazards' aanpak, en integreer dit met BIO's risico gebaseerde methodologie.

3.4. Naleving van BIO en NIS2 Controles

BIO

- Toegangsbeheer: Leverancier implementeert sterke authenticatie (bijv. multi-factor authenticatie) en op rollen gebaseerde toegangscontroles (RBAC) voor alle systemen en gegevens, volgens het principe van minimale bevoegdheden.

- Gegevensbescherming: Leverancier versleutelt gevoelige gegevens in rust en tijdens verzending met industriestandaard protocollen (bijv. AES-256, TLS 1.3)

[TLS1.2 is nog betrouwbaar, maar TLS 1.3 is toekomstbestendiger.]

- Incidentbeheer: Leverancier stelt een proces voor beveiligingsincidentbeheer op om incidenten te detecteren, hierop te reageren en binnen afgesproken termijnen te rapporteren, in lijn met BIO vereisten.

- Audit en Logging: Leverancier houdt uitgebreide auditlogs bij voor alle kritieke systemen, met bewaartermijnen in overeenstemming met BIO (doorgaans 6-12 maanden).

- Fysieke en Omgevingsbeveiliging: Leverancier beveiligt datacenters (on-prem of cloud) met fysieke toegangscontroles, milieubescherming (bijv. brand, overstroming) en redundantiemaatregelen.

NIS2 Aanvullingen:

- Strengere Toegangsbeheer: Leverancier implementeert verplichte multi-factor authenticatie (MFA) of continue authenticatie voor toegang tot kritieke systemen en gegevens, en gebruikt netwerksegmentatie om risico's te beperken, zoals voorgeschreven door NIS2.

- Geavanceerde Encryptie: Leverancier ontwikkelt en documenteert specifieke beleidsregels voor het gebruik van cryptografie, inclusief encryptieprotocollen, om gegevens te beschermen tegen ransomware en ongeautoriseerde toegang.

- Incidentrapportage: Leverancier meldt significante cyberincidenten binnen 24 uur aan de bevoegde autoriteit of het Computer Security Incident Response Team (CSIRT), gevolgd door een gedetailleerd rapport binnen 72 uur en een eindrapport binnen een maand, zoals vereist door NIS2. Incidenten omvatten verstoringen die de continuïteit van diensten aanzienlijk beïnvloeden, gebaseerd op factoren zoals het aantal getroffen personen, de duur van de verstoring, en financiële verliezen.

- Geautomatiseerde Monitoring: Leverancier gebruikt geautomatiseerde monitoring- en loggingtools om verdachte activiteiten te detecteren en snelle respons mogelijk te maken. Centrale logopslag moet beveiligd zijn tegen ongeautoriseerde toegang en regelmatig worden geback-upt.

Praktisch: Leverancier combineert BIO controles met NIS2's vereisten door een geïntegreerd beveiligingsdashboard te implementeren dat real-time monitoring en rapportage ondersteunt, geschikt voor zowel on-prem als cloudomgevingen.

3.5. Cloudspecifieke Eisen

BIO: Voor clouddiensten, voldoe aan aanvullende BIO-controles (in lijn met ISO27017):

- Leverancier zorgt voor duidelijke scheiding van verantwoordelijkheden tussen leverancier en klant in gedeelde verantwoordelijkheidsmodellen.

- Leverancier gebruikt cloudproviders met certificeringen zoals ISO27001, CSA STAR of gelijkwaardig, en verifieert naleving van Nederlandse vereisten voor gegevenslocatie.

- Leverancier implementeert mechanismen voor gegevensback-up en herstel om beschikbaarheid te waarborgen, met gedefinieerde hersteltijd (RTO) en herstelpuntdoelstellingen (RPO).

- Leverancier maakt veilige API-toegang mogelijk en voert regelmatig kwetsbaarheidsscans uit.

NIS2 Aanvullingen: voor cloud computing-diensten, zoals gedefinieerd in NIS2, implementeert leverancier specifieke technische en organisatorische maatregelen, zoals veilige configuraties voor cloudinfrastructuur en actieve detectie van kwetsbaarheden in cloudgebaseerde systemen. Leverancier zorgt voor compliance met de NIS2-uitvoeringsverordening voor cloudproviders, zoals vastgelegd in Verordening C(2024) 7151, die technische en methodologische eisen specificeert.

Praktisch: Leverancier gebruikt cloudbeveiligingsoplossingen die continue nalevingscontroles bieden (bijv. Orca Security's platform met 150+ frameworks) om zowel BIO- als NIS2-vereisten te waarborgen.

3.6. Personeelsbeveiliging

BIO: Leverancier voert achtergrondonderzoeken en beveiligingstrainingen uit voor al het personeel dat gevoelige gegevens of systemen behandelt. Leverancier handhaaft vertrouwelijkheidsovereenkomsten.

NIS2 Aanvullingen: Leverancier implementeert verplichte, regelmatige trainingen over cyberhygiëne en beveiligingsrisico's voor alle medewerkers, inclusief procedures voor toegang tot gevoelige gegevens. NIS2 benadrukt de verantwoordelijkheid van het management om deze trainingen te waarborgen en een cultuur van cyberbewustzijn te bevorderen.

Praktisch: Leverancier ontwikkelt een jaarlijks trainingsprogramma dat zowel BIO's eisen voor bewustwording als NIS2's focus op managementverantwoordelijkheid en basis cyberhygiëne omvat.

3.7. Beveiliging van Toeleveringsketen

BIO: Leverancier zorgt ervoor dat onderaannemers en externe leveranciers voldoen aan BIO-vereisten, met contractuele verplichtingen voor beveiliging en regelmatige nalevingsaudits. Leverancier brengt de toeleveringsketen in kaart en monitort deze om risico's van externe partijen te mitigeren.

NIS2 Aanvullingen: Leverancier implementeert specifieke beveiligingsmaatregelen voor de toeleveringsketen, inclusief het beoordelen van de beveiligingsniveaus van directe leveranciers en het opstellen van contracten die NIS2-conformiteit vereisen. Leverancier moet kwetsbaarheden in de toeleveringsketen identificeren en aanpakken, met name voor digitale diensten zoals cloud- en beheerde beveiligingsdiensten.

Praktisch: Leverancier gebruikt tools zoals software bill of materials (SBOM) en software composition analysis (SCA) om kwetsbare derde partij-componenten te detecteren, zoals aanbevolen door NIS2.

Voor de PNB zijn de eisen vanuit NIS2, BIO en ISO27001 sterk verweven. NIS2 legt de nadruk op ketenverantwoordelijkheid en zorgplicht, BIO biedt een overheidspecifiek normenkader dat aansluit bij ISO 27001, en ISO 27001 biedt een gestructureerde aanpak voor een ISMS.

In de IT-keten moet de provincie risico's systematisch beheren, leverancierscontracten versterken, en moderne standaarden zoals TLS 1.3 adopteren. *Hoewel TLS 1.2 nog betrouwbaar is, is een overgang naar TLS 1.3 wenselijk voor toekomstbestendigheid*. Door deze kaders te integreren en leveranciers (inclusief cloud-providers) te verplichten tot aantoonbare beveiligingsmaatregelen, kunnen provincies voldoen aan de eisen en wensen van NIS2 en BIO.

- Inventarisatie van de IT-keten: Breng alle leveranciers, inclusief SaaS, PaaS en IaaS providers, in kaart en beoordeel hun beveiligingsniveau.
- Contractuele afspraken: Stel SLA's op met expliciete eisen voor cybersecurity, zoals ISO27001-compliance, gebruik van TLS 1.3, en incidentrapportage.
- Risicoanalyse: Voer regelmatig ketenbrede risicoanalyses uit, met specifieke aandacht voor cloud-diensten en zwakke schakels.
- Training: Organiseer trainingen voor bestuurders en medewerkers over ketenrisico's en NIS2-eisen.
- Audits en monitoring: Implementeer een proces voor periodieke audits van leveranciers en gebruik tools voor continue monitoring van de keten.
- Transitie naar TLS 1.3: Plan een gefaseerde overgang van TLS 1.2 naar TLS 1.3 voor alle ketencommunicatie.

3.8. Continue Monitoring en Verbetering

BIO: Leverancier voert regelmatig beveiligingsbeoordelingen uit, inclusief penetratietesten en kwetsbaarheidsscans. Leverancier voert jaarlijkse audits uit van het ISMS en BIO-naleving. Leverancier hanteert een Plan-Do-Check-Act (PDCA)-cyclus voor continue verbetering.

NIS2 Aanvullingen: Leverancier implementeert continue monitoring van netwerken en systemen om cyberdreigingen snel te detecteren, zoals vereist door NIS2. Leverancier voert regelmatige audits uit (zowel op locatie als extern) en rapporteert nalevingsstatus aan bevoegde autoriteiten. Leverancier ontwikkelt procedures voor kwetsbaarheidsbeheer en openbaarmaking, inclusief een bijdrage aan de EU-kwetsbaarheidsdatabase beheerd door ENISA.

Praktisch: Leverancier gebruikt geautomatiseerde tools zoals GFI LanGuard of Orca Security voor netwerkzichtbaarheid, patchbeheer en nalevingsrapportages die zowel BIO- als NIS2-vereisten dekken.

3.9. Wettelijke en Regelgevende Naleving

BIO: Leverancier voldoet aan relevante Nederlandse en EU-regelgeving, inclusief de AVG (GDPR) voor persoonsgegevens en NCSC-richtlijnen.

NIS2 Aanvullingen: Leverancier zorgt voor naleving van de Cyberbeveiligingswet (Cbw) en andere nationale implementaties van NIS2. Leverancier moet significante incidenten melden en samenwerken met nationale CSIRT's en de EU-CyCLONe voor grensoverschrijdende incidentrespons. (Niet-naleving kan leiden tot boetes tot €10 miljoen of 2% van de wereldwijde jaaromzet voor essentiële entiteiten, en €7 miljoen of 1,4% voor belangrijke entiteiten).

Praktisch: Leverancier sluit gegevensverwerkingsovereenkomsten (DPA's) af en stelt een proces in voor snelle incidentrapportage conform NIS2-tijdlijnen.

3.10. Interoperabiliteit en Rapportage

BIO: Leverancier levert regelmatig rapportages over beveiligingsprestaties in een formaat dat compatibel is met de monitoringsystemen van de contracterende organisatie. Leverancier zorgt voor interoperabiliteit met overheidsstandaarden.

NIS2 Aanvullingen: Leverancier zorgt voor gestroomlijnde rapportageprocessen voor incidenten en nalevingsstatus, compatibel met nationale en EU-autoriteiten. Leverancier werkt samen met de NIS Cooperation Group en CSIRT's voor informatie-uitwisseling en grensoverschrijdende samenwerking.

Praktisch: Leverancier implementeert een gecentraliseerd rapportagesysteem dat zowel BIO-auditlogs als NIS2-incidentrapportages ondersteunt, met exporteerbare rapporten voor auditors.

3.11. Bedrijfscontinuïteit en Crisisbeheer

BIO: Leverancier ontwikkelt back-up- en herstelmechanismen om beschikbaarheid te waarborgen, met gedefinieerde RTO en RPO.

NIS2 Aanvullingen: Leverancier stelt uitgebreide plannen op voor bedrijfscontinuïteit, crisisbeheer en disaster recovery, inclusief veilige back-ups en procedures voor snelle gegevensherstel na incidenten zoals ransomware of systeemuitval. Leverancier voert regelmatige tests uit om de effectiviteit van deze plannen te valideren.

Praktisch: Leverancier implementeert geautomatiseerde back-upsystemen en test herstelprocedures minimaal jaarlijks, met rapportages die voldoen aan zowel BIO- als NIS2-auditvereisten.

4. RELATIE VAN DE RICHTLIJN MET ANDERE DOCUMENTEN

Proces	Aard gegevens
Informatiebeveiligingsbeleid	Kader stellend
BIO	Kader stellend
NEN-ISO 27001	Kader stellend
NEN-ISO 27002	Kader stellend

5. RELATIE VAN DE RICHTLIJN MET VERSCHILLENDE WET EN REGELGEVING

Wet & Regelgeving	Verwijzing
NEN-ISO 27001	
NEN-ISO 27002	
BIO	

6. ROLLEN EN VERANTWOORDELIJKHEDEN

Rol	Verantwoordelijkheid
Chief Information Security Officer (CISO)	- Opstellen en onderhouden van deze richtlijn
Information Security Officer (ISO)	- Ondersteuning bij de implementatie
Opdrachtnemer ICT-beheer	- Implementatie van de maatregelen zoals benoemd in deze richtlijn - Rapporteren van incidenten in relatie tot deze richtlijn bij de ISO
Medewerkers Provincie Noord-Brabant	- Het naleven van de maatregelen zoals opgenomen in deze richtlijn