Informatiebeveiligingsbeleid 2026 - 2028

Documentinformatie	
Versie	1.0
Status	Definitief
Datum	12-8-2026
Classificatie	Openbaar

Inhoudsopgave

1. Informatiebeveiligingsbeleid

1.1 Doel

Dit beleidsdocument beschrijft het strategisch informatiebeveiligingsbeleid van BIDN voor de jaren 2026 tot en met 2028. Het beleid is richtinggevend en kaderstellend voor de bescherming van informatie, informatiesystemen, gegevensverwerkingen en ondersteunende middelen binnen de organisatie.

Het beleid vormt de strategische basis voor onderliggende uitvoeringsregelingen, procedures, normen, werkinstructies en maatregelen. De concrete taken, verantwoordelijkheden en bevoegdheden voor informatiebeveiliging zijn uitgewerkt in de Uitvoeringsregeling Informatiebeveiligingsbeleid.

1.1.1 Geldigheidsduur

Dit beleid is vastgesteld op 12-08-2026 door de Directeur-bestuurder als eindverantwoordelijke voor BIDN gegevensverwerking. Het beleid wordt jaarlijks beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van security impact assessments (SIA's) en/of beveiligingsincidenten) kan de Directeur-bestuurder besluiten tot een tussentijdse herziening.

1.2 Wat is informatiebeveiliging

Informatiebeveiliging is het treffen, onderhouden en aantoonbaar beheersen van een samenhangend pakket van maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen. Informatiebeveiliging wordt risico gestuurd ingericht en onderhouden binnen het Information Security Management System (ISMS). Informatiebeveiliging is daarmee geen uitsluitend technische activiteit. Het betreft een samenhang van governance, processen, mensen, technologie, gegevens, leveranciers, ketens en fysieke en digitale omgevingen.

1.3 Ambitie en visie

BIDN verwerkt en faciliteert gegevensuitwisseling in ketens waarin betrouwbaarheid, rechtmatigheid en continuïteit essentieel zijn. De ambitie is om informatiebeveiliging zodanig in te richten dat opdrachtgevers, afnemers, burgers, medewerkers en ketenpartners erop kunnen vertrouwen dat informatie passend wordt beschermd en dat risico's aantoonbaar worden beheerst.

BIDN hanteert daarbij een risico gestuurde en aantoonbare aanpak. Kwetsbaarheden, dreigingen, incidenten, auditbevindingen en wijzigingen in wet- en regelgeving worden gebruikt om beleid, maatregelen en werkwijzen periodiek te verbeteren. Waar uit risicoanalyse, wetgeving, contractuele verplichtingen of classificatie volgt dat aanvullende maatregelen nodig zijn, worden deze opgenomen in het ISMS en de relevante uitvoeringsdocumenten.

2. Strategisch beleid

2.1 Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, organisatieonderdelen, informatiesystemen, informatie, gegevensverwerkingen, medewerkers en middelen van BIDN. Het beleid geldt ongeacht locatie, tijdstip, gebruikte apparatuur of wijze van toegang.

De scope omvat uitbestede diensten, cloud- en SaaS-diensten, ketenkoppelingen, gegevensuitwisselingen, ontwikkel-, test-, acceptatie- en productieomgevingen voor zover deze worden gebruikt voor of invloed hebben op de informatievoorziening van BIDN.

Dit beleid vormt een algemene basis en dekt aanvullende beveiligingseisen uit wetgeving, overeenkomsten en ketenafspraken voor zover deze binnen de scope van BIDN vallen. Specifieke eisen worden nader uitgewerkt in onderliggende documenten en het controlregister.

2.2 Normenkader en beleidsarchitectuur

BIDN baseert het ISMS op de actuele versie van NEN-EN-ISO/IEC 27001. Daarbij worden de overheidsmaatregelen vanuit de Baseline Informatiebeveiliging Overheid versie (BIO) toegevoegd en uitgewerkt. De koppeling tussen beleidsuitgangspunten, BIO-maatregelen, interne beheersmaatregelen en bewijsvoering wordt beheerd in het controlregister en in de relevante uitvoeringsdocumenten.

Beleidsniveau	Doel	Document
Strategisch beleid	Richtinggevende kaders en uitgangspunten voor informatiebeveiliging.	Beleid Informatiebeveiliging 2026-2028.
Uitvoeringsregeling	Uitwerking van rollen, verantwoordelijkheden, governance, besluitvorming en uitvoering.	Uitvoeringsregeling Informatiebeveiligingsbeleid 2026-2028
Procedures en normen	Concrete werkwijzen, eisen en processtappen.	Procedure beveiligingsincidenten, wijzigingsproces, toegangsbeheer, logging en monitoring, SSD/SIA-proces.
Registraties en bewijsvoering	Aantoonbaarheid van uitvoering en werking.	Risicoregister, controlregister, auditdossier, incidentregister, verbeterregister.
Beleidsniveau	Doel	Document

2.3 Strategische uitgangspunten

De volgende uitgangspunten zijn leidend voor de inrichting en uitvoering van informatiebeveiliging binnen BIDN:

1. Informatiebeveiliging is risico gestuurd. Maatregelen worden gekozen op basis van risico's, wettelijke verplichtingen, contractuele eisen, classificatie en organisatorische doelstellingen, zoals vastgelegd in het Koersdocument en de jaarplannen.
2. De Directeur-bestuurder is bestuurlijk verantwoordelijk voor de inrichting, sturing en borging van informatiebeveiliging. De Directeur-bestuurder stelt kaders vast, bepaalt de risicobereidheid en ziet toe op werking en opvolging.
3. Proceseigenaren in de lijn worden geacht dit beleid te kennen en zijn verantwoordelijk voor de beheersing van informatiebeveiligingsrisico's binnen hun processen en systemen.
4. De Security Manager coördineert, adviseert, bewaakt en rapporteert over informatiebeveiliging en ondersteunt Directeur-bestuurder en proceseigenaren bij besluitvorming.
5. Informatiebeveiliging is onderdeel van ontwerp, ontwikkeling, verwerving, wijziging, beheer en beëindiging van processen, systemen en diensten.
6. Toegang tot informatie en systemen wordt verleend op basis van noodzaak, proportionaliteit, autorisatie en periodieke beoordeling.
7. Productieomgevingen zijn logisch en/of fysiek gescheiden van ontwikkel-, test- en acceptatieomgevingen. Toegang tot productieomgevingen wordt beperkt, gemonitord en periodiek beoordeeld.
8. Het risico op verlies, ongeautoriseerde wijziging of niet-beschikbaarheid van informatie wordt beperkt tot een acceptabel niveau. Waar nodig worden back-up-, herstel- en continuïteitsmaatregelen getroffen.
9. Beveiligingsincidenten, kwetsbaarheden, datalekken, auditbevindingen en afwijkingen worden geregistreerd, beoordeeld, opgevolgd en gebruikt als input voor verbetering.
10. Medewerkers zijn verantwoordelijk voor zorgvuldig gebruik van informatie en middelen, naleving van beleid en procedures en tijdige melding van incidenten, kwetsbaarheden en ongewenste situaties.
11. Informatiebeveiliging maakt deel uit van afspraken met ketenpartners, leveranciers en dienstverleners.
12. Het ISMS wordt periodiek beoordeeld en verbeterd volgens de plan-do-check-act-systematiek.

2.4 Governance, rollen en verantwoordelijkheden

Rollen, verantwoordelijkheden en bevoegdheden voor informatiebeveiliging zijn vastgelegd in de 'Uitvoeringsregeling Informatiebeveiligingsbeleid'. De actuele personele invulling van rollen wordt beheerd in het document 'Organisatie van de informatiebeveiliging en Privacy'.

2.5 Risico gestuurde aanpak

BIDN voert periodiek en bij relevante wijzigingen risicoanalyses uit om inzicht te krijgen in bedreigingen, kwetsbaarheden, impact en waarschijnlijkheid. Daarbij wordt rekening gehouden met mensen, processen, technologie, gegevens, organisatie, omgeving, leveranciers en ketens.

Risico's worden geregistreerd, beoordeeld en behandeld. Restrisico's worden expliciet geaccepteerd door het daarvoor bevoegde managementniveau. De uitkomsten van risicoanalyses zijn input voor jaarplannen, verbetermaatregelen, audits, wijzigingsbeoordelingen en directiebeoordelingen.

BIDN hanteert een minimaal uitgangspunt voor de inrichting van informatiebeveiliging, tenzij uit wetgeving, contractuele verplichtingen, risicoanalyse of classificatie volgt dat aanvullende maatregelen noodzakelijk zijn.

2.6 Security-by-design en wijzigingsbeheer

Informatiebeveiliging wordt meegenomen bij ontwerp, ontwikkeling, aanschaf, wijziging en beheer van processen, applicaties, koppelingen en infrastructuur. Voor wijzigingen met impact op informatiebeveiliging wordt een Security Impact Assessment uitgevoerd of wordt een gelijkwaardige risicobeoordeling vastgelegd.

Voor Secure Software Development wordt gebruikgemaakt van passende normen en richtlijnen, waaronder de SSD-beveiligingseisen van het Centrum Informatiebeveiliging en Privacy, de OWASP Application Security Verification Standard, de OWASP Top 10 waar passend, en relevante NCSC-richtlijnen. De toepassing van deze eisen wordt geborgd via het wijzigingsproces.

Voor het veilig inrichten van het IT-landschap wordt gebruik gemaakt van de Critical Security Controls van het Center for Information Security (CIS-controls).

2.7 Incidenten, kwetsbaarheden en continu verbeteren

Beveiligingsincidenten, kwetsbaarheden, inbreuken, afwijkingen en datalekken worden volgens de daarvoor vastgestelde procedures gemeld, geregistreerd, beoordeeld en opgevolgd. Lessen uit incidenten en kwetsbaarheden worden gebruikt om maatregelen, procedures, bewustwording en technische inrichting te verbeteren.

BIDN gebruikt interne incidentregistraties, auditbevindingen, dreigingsinformatie, signaleringen van ketenpartners en relevante externe dreigingsbeelden als input voor de actualisatie van beleid, jaarplannen en beheersmaatregelen.

2.8 Ketenpartners, leveranciers en uitbestede diensten

Informatiebeveiliging maakt onderdeel uit van afspraken met opdrachtgevers, afnemers, ketenpartners, leveranciers en dienstverleners. Eisen aan beschikbaarheid, integriteit, vertrouwelijkheid, continuïteit, logging, monitoring, incidentmelding, auditrechten en gegevensbescherming worden waar relevant vastgelegd in overeenkomsten, verwerkersafspraken, ketenafspraken, inkoopvoorwaarden of technische aansluitvoorwaarden.

Leveranciers en uitbestede diensten worden risico gestuurd beoordeeld. Daarbij wordt rekening gehouden met de aard van de dienstverlening, de gevoeligheid van informatie, afhankelijkheden in ketens en de mate waarin de leverancier invloed heeft op de informatievoorziening van BIDN.

2.9 Bewustwording en naleving

BIDN bevordert kennis en bewustzijn van informatiebeveiliging actief. Medewerkers worden geïnformeerd en periodiek getraind in het veilig omgaan met informatie, systemen, middelen, persoonsgegevens en meldprocedures. Van medewerkers wordt verwacht dat zij zorgvuldig handelen, beleid en procedures naleven en beveiligingsincidenten, kwetsbaarheden of ongewenste situaties tijdig melden.

Naleving van dit beleid wordt ondersteund door communicatie, training, procedures, controles, rapportages en periodieke beoordeling. Afwijkingen worden vastgelegd, beoordeeld en waar nodig opgevolgd met corrigerende of preventieve maatregelen.

3. Controle en verantwoording

3.1 ISMS en directiebeoordeling

Het ISMS borgt dat informatiebeveiliging planmatig wordt ingericht, uitgevoerd, gecontroleerd en verbeterd. De Directeur-bestuurder laat minimaal tweemaal per jaar een directiebeoordeling van het ISMS uitvoeren conform de actuele ISO 27001-systematiek.

In de directiebeoordeling worden ten minste de status van risico's, incidenten, auditbevindingen, verbetermaatregelen, prestaties van het ISMS, wijzigingen in context en relevante dreigingsontwikkelingen beoordeeld. Besluiten en acties uit de directiebeoordeling worden vastgelegd en gemonitord.

3.2 Audit, assurance en rapportage

BIDN verantwoordt zich over informatiebeveiliging via interne controles, directiebeoordelingen, audits en externe assurance waar dit wettelijk, contractueel of bestuurlijk is vereist. Jaarlijks wordt vastgesteld welke onderwerpen, processen, stelsels, controls en maatregelen in scope zijn voor toetsing.

De resultaten van interne controles, audits, directiebeoordelingen en externe assurance worden gerapporteerd aan de Directeur-bestuurder. De Directeur-bestuurder bewaakt dat bevindingen, restrisico's en verbetermaatregelen tijdig en aantoonbaar worden opgevolgd.

De resultaten van de jaarlijkse externe audit worden per wettelijk stelsel gedeeld met de betreffende opdrachtgevers en stelselverantwoordelijken. Jaarlijks wordt aan de minister van Sociale Zaken en Werkgelegenheid (SZW) gerapporteerd over de werking van de informatiebeveiliging van alle informatiediensten en producten, op basis van een NOREA-audit. Voor de informatiediensten binnen het kader van de Jeugdwet en de Wmo ontvangt de Vereniging van Nederlandse Gemeenten (VNG) een auditrapport.

De verantwoording over informatiebeveiliging wordt daarnaast opgenomen in de verklaring informatiebeveiliging in het jaarverslag. Details over scope, normenkader, planning, bewijsvoering en opvolging worden uitgewerkt in het auditplan, controlregister en verantwoordingsdossier.

3.3 Beoordeling en actualisatie van dit beleid

Dit beleid wordt minimaal jaarlijks beoordeeld en daarnaast tussentijds wanneer wijzigingen in wet- en regelgeving, BIO, ISO 27001, dreigingsbeeld, organisatie, dienstverlening, technologie of auditbevindingen daartoe aanleiding geven.

De Securitymanager bewaakt de actualiteit van dit beleid en adviseert over noodzakelijke wijzigingen. De Directeur-bestuurder stelt het beleid vast. De uitvoering en werking van dit beleid worden beoordeeld via het ISMS, de directiebeoordeling, interne controles, audits en rapportages aan de Directeur-bestuurder.