REGIONALE BELASTING GROEP

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 1065

11 mei 2026

Officiële uitgave van de gemeenschappelijke regeling Regionale Belasting Groep

Informatiebeveiligingsbeleid 2026

Inleiding

De Regionale Belasting Groep (RBG) opereert in een volledig digitale werkelijkheid. De uitvoering van haar wettelijke taken is in hoge mate afhankelijk van informatiesystemen en digitale informatiestromen. Vrijwel alle informatie binnen de organisatie is digitaal beschikbaar, wordt digitaal uitgewisseld en grotendeels in de cloud verwerkt. Medewerkers maken dagelijks gebruik van mobiele en vaste digitale werkmiddelen die via beveiligde verbindingen toegang bieden tot bedrijfskritische applicaties. Deze digitale inrichting maakt een efficiënte en toegankelijke dienstverlening mogelijk, maar brengt tegelijkertijd nieuwe en toenemende risico's met zich mee.

Voor een betrouwbare en continue uitvoering van de dienstverlening is het essentieel dat informatie en informatiesystemen voldoen aan de eisen van **beschikbaarheid, integriteit en vertrouwelijkheid,** Verstoringen, datalekken of uitval van systemen kunnen directe gevolgen hebben voor burgers, deelnemers en de bedrijfscontinuïteit van de RBG.

Tegelijkertijd staat informatiebeveiliging nationaal en internationaal nadrukkelijk onder druk. Cyberdreigingen nemen in omvang, complexiteit en impact toe. Overheden, vitale organisaties en publieke instellingen worden in toenemende mate geconfronteerd met cyberaanvallen, waaronder ransomware en grootschalige datalekken. Recente incidenten binnen de rijksoverheid onderstrepen dat ook publieke organisaties kwetsbaar zijn en dat structurele aandacht voor digitale veiligheid onmisbaar is.

Deze ontwikkelingen hebben geleid tot een duidelijke bestuurlijke opdracht vanuit de landelijke overheid. Zowel de Tweede Kamer als het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) benadrukken dat overheden hun digitale weerbaarheid moeten versterken en informatiebeveiliging structureel moeten verankeren in beleid, governance en uitvoering.

Daarbij komt dat geopolitieke spanningen de urgentie verder vergroten. Digitale dreigingen worden steeds vaker ingezet als strategisch instrument in internationale machtsverhoudingen. Europese overheden en publieke organisaties vormen daarbij expliciet een doelwit. Dit vraagt om een bewuste omgang met afhankelijkheden, in het bijzonder ten aanzien van digitale infrastructuur, cloudvoorzieningen en technologieën van buiten Europa.

De **Nederlandse Digitaliseringsstrategie (NDS)** vormt een van de pijlers van het kabinetsbeleid op digitalisering en is gericht op het gezamenlijk versnellen van digitalisering binnen alle bestuurslagen

Een belangrijk speerpunt binnen de NDS is **digitale soevereiniteit**. De Nederlandse overheid definieert dit niet als volledige technologische autonomie, maar als het **vermogen om zelf bewuste keuzes te maken en regie te houden** over digitale infrastructuur, data en technologiepartners

Positionering
De **Regionale Belasting Groep (RBG)** is in hoge mate afhankelijk van digitale informatiesystemen voor de uitvoering van haar wettelijke taken. Informatiebeveiliging is daarom een **strategisch organisatie brede verantwoordelijkheid** en een randvoorwaarde voor betrouwbare publieke dienstverlening.

Dit beleid beschrijft **op hoofdlijnen**:

- Hoe de RBG invulling geeft aan haar wettelijke zorgplichten;
- Hoe verantwoordelijkheden zijn belegd op **bestuurlijk** en **operationeel niveau**;
- Hoe informatiebeveiliging bijdraagt aan continuïteit, rechtmatigheid en vertrouwen.

Dit document vormt het kaderstellend beleidsdocument; nadere uitwerking vindt plaats in tactische en operationele procedures.

Doel van informatiebeveiliging

Het informatiebeveiligingsbeleid heeft tot doel duidelijke kaders te stellen waarbinnen de werking van onze informatiesystemen en de (geautomatiseerde) uitwisseling van informatie op een betrouwbare en gecontroleerde wijze wordt ingericht. Hiermee waarborgen wij de **beschikbaarheid, integriteit** en **vertrouwelijkheid** van zowel onze systemen als de gegevens die binnen en buiten de organisatie worden gedeeld.

Deze kaders hebben niet uitsluitend betrekking op digitale informatiesystemen. Zij omvatten eveneens de beveiliging van **niet-digitale gegevensdragers**, evenals de **fysieke beveiliging** van onze gebouwen, werkplekken en medewerkers. Informatiebeveiliging wordt daarmee als een integraal onderdeel van de bedrijfsvoering beschouwd, waarbij zowel technische als organisatorische maatregelen bijdragen aan een veilige en stabiele werkomgeving.

Wettelijk en normatief kader
Baseline Informatiebeveiliging Overheid

De BIO is het **verplichte normenkader** voor informatiebeveiliging binnen de overheid.
De RBG werkt risicogebaseerd volgens BIO principes, waaronder:

- Classificatie van informatie;
- Passende technische en organisatorische maatregelen;
- Incidentmanagement en logging;
- Continue verbetering via PDCA.

NIS2 richtlijn

De NIS2 richtlijn scherpt de eisen aan voor:

- Bestuurlijke verantwoordelijkheid;
- Zorgplicht voor digitale weerbaarheid;
- Aantoonbare governance en toezicht;
- Keten- en leveranciersbeveiliging.

De RBG anticipeert hierop door BIO conform werken expliciet te verankeren in bestuur en directie.

Cyberbeveiligingswet (CBW)
De CBW vormt de nationale implementatie van NIS2.
De BIO (richting BIO 2.0) fungeert als **sectorspecifieke invulling van de zorgplicht** voor overheidsorganisaties.

De RBG beschouwt de CBW als richtinggevend kader voor haar informatiebeveiligingsstrategie.

Nederlandse Digitaliseringsstrategie (NDS)

De NDS benadrukt dat digitale dienstverlening moet voldoen aan:

- Betrouwbaarheid,
- Veiligheid
- Transparantie

Informatiebeveiliging en privacy zijn daarbij **randvoorwaardelijk** voor digitalisering binnen de RBG.

Scope van het beleid

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om:

- alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, kennis)
- alle mogelijke informatiedragers (papier, elektronisch, foto, film, USB, SD kaart, beeldscherm etc.)
- alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, netwerken, databases, hardware, bijbehorende bedrijfsmiddelen)
- toegang tot gebouw en ruimtes
- het gebruik van apparatuur
- menselijk handelen en processen.

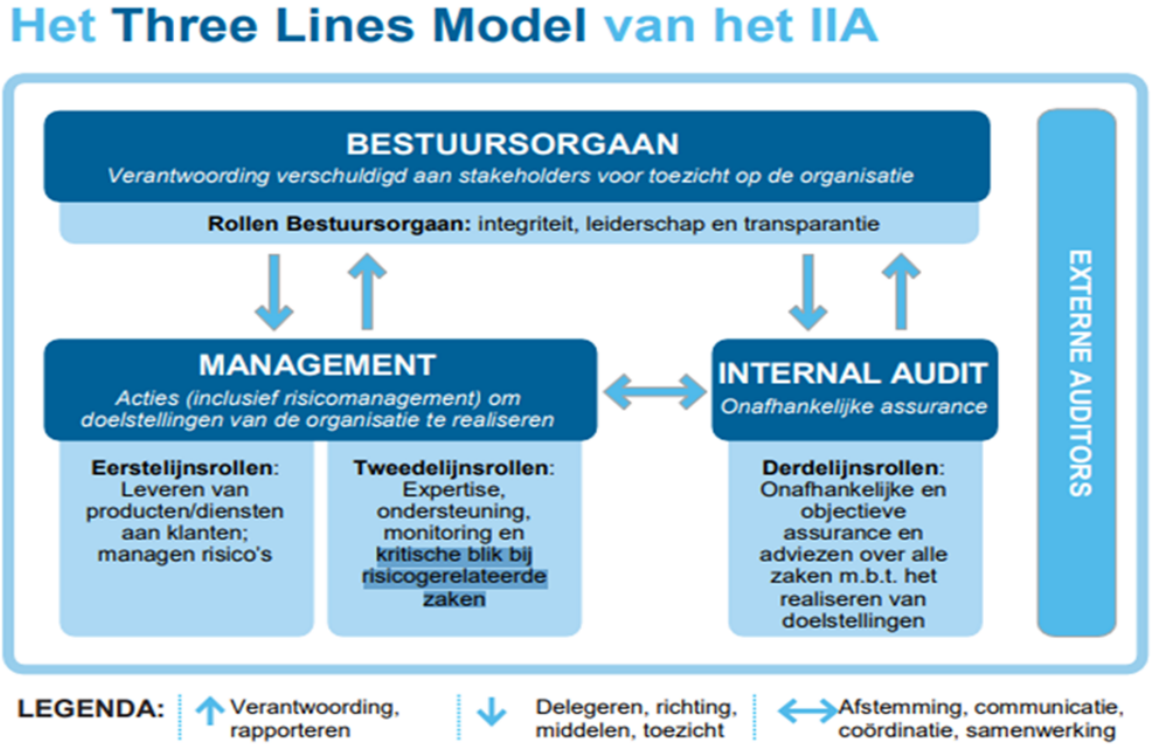
De meeste beveiligingsincidenten ontstaan niet door falende techniek, maar door menselijk handelen en een gebrek aan bewustzijn binnen de organisatie. Daarom richt de RBG zich niet alleen op technische maatregelen, maar juist ook op het versterken van kennis, alertheid en verantwoordelijk gedrag van alle medewerkers.

De reikwijdte van het informatiebeveiligingsbeleid omvat alle bedrijfsfuncties, ondersteunende middelen en informatie van de RBG in de breedste zin van het woord. Het beleid is van toepassing op alle ruimten binnen het kantoorpand, op alle apparatuur en programmatuur, en op alle informatie en gegevens die

door de RBG worden gebruikt of verwerkt. Zo borgen we dat informatieveiligheid een integraal onderdeel is van onze gehele organisatie.

1. Organieke inbedding

De organiek inbedding van taken en verantwoordelijkheden is gebaseerd op het Three Lines Model:



Dagelijks Bestuur

- Stelt het informatiebeveiligingsbeleid vast;
- Bepaalt de risicobereidheid van de organisatie;
- Ziet toe op naleving van wet- en regelgeving (BIO, NIS2, CBW, AVG);
- Ontvangt jaarlijks een rapportages over:
  - Beveiligingsrisico's;
  - Incidenten en datalekken;
  - Voortgang van verbetermaatregelen.

Onder NIS2/CBW wordt informatiebeveiliging expliciet als **bestuurlijke verantwoordelijkheid** gezien

Directie
De directie van de RBG draagt de **integrale operationele verantwoordelijkheid** voor informatiebeveiliging en:

- Vertaalt bestuurlijk beleid naar uitvoering;
- Borgt implementatie van BIO maatregelen;
- Zorgt voor voldoende middelen, capaciteit en prioritering;
- Is eindverantwoordelijk voor:
  - Operationele uitvoering van het Informatiebeveiligingsbeleid
  - Incidentafhandeling;
  - Herstelmaatregelen;
  - Structurele verbeteringen.

Teammanagers
Zijn verantwoordelijk voor de beveiliging en privacy binnen hun processen:

- Voeren risico gebaseerde maatregelen uit conform de BIO;

- Opleidingen en bewustwording medewerkers
- Signaleren en escaleren risico's en incidenten tijdig.

Chief Information & Security Officer CISO:

- Adviseert bestuur en directie;
- Opstellen Informatiebeveiligingsbeleid;
- Bewaakt samenhang tussen informatiebeveiliging, privacy en continuïteit;
- Coördineert risicomanagement en incidentmanagement;
- Rapporteert periodiek over dreigingen en beveiligingsstatus;
- Controle op naleving van het beleid en maatregelen.

De Regionale Belasting Groep heeft functionarissen aangesteld welke zijn opgenomen in het functieboek voor:

Chief Information & Security Officer (CISO)
Privacy Officer (PO)
Functionaris Gegevensbescherming (FG)

2. Uitwerking beleid

De RBG hanteert de volgende uitgangspunten voor de uitvoering van haar beleid:

- Risico gebaseerd beveiligen (BIO);
- Privacy en security by design;
- Need to know / least privilege;
- Ketenverantwoordelijkheid richting leveranciers;
- **Continue verbetering** en aantoonbaarheid via ISMS

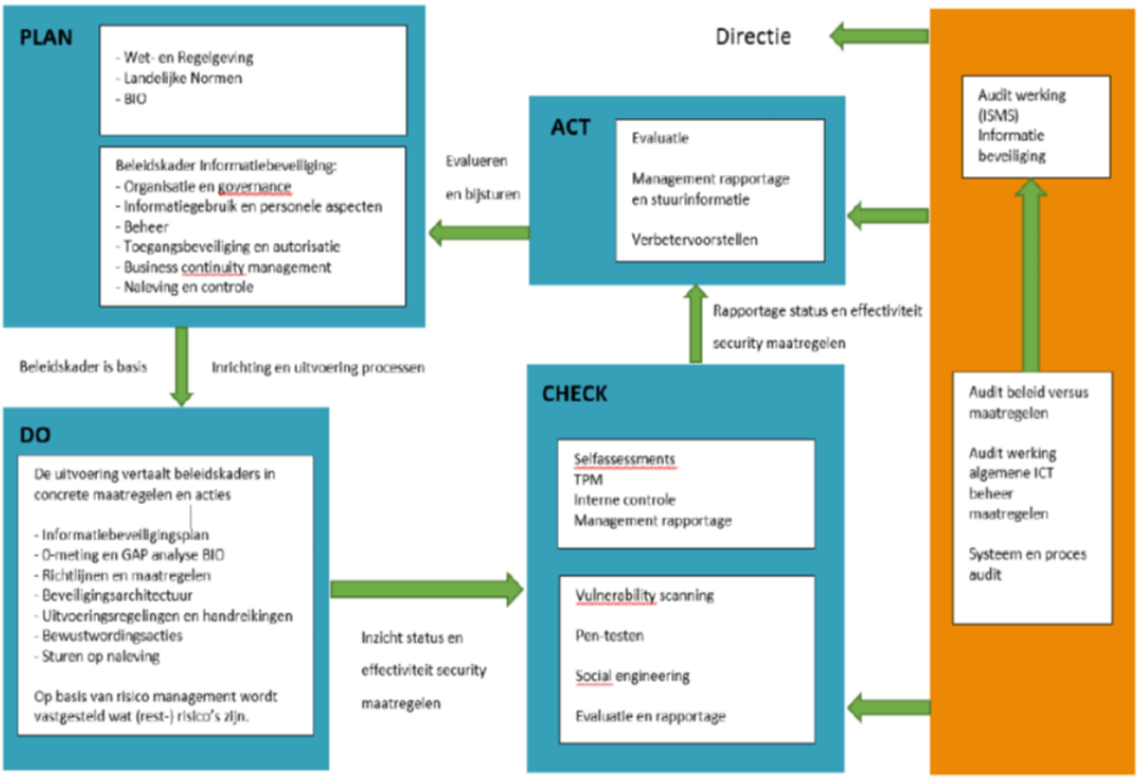
Jaarlijks wordt op basis van het beveiligingsbeleid een risico of knelpunten analyse uitgevoerd op binnen de scope vallende onderdelen. Naar aanleiding van de geconstateerde knelpunten wordt een uitvoeringsplan (informatiebeveiligingsplan) opgesteld. Hierin wordt de implementatie van het beleid, richtlijnen, procesbeschrijvingen, procedures en technische maatregelen met betrekking tot informatiebeveiliging beschreven. De implementatie en handhaving hiervan is primair de verantwoordelijkheid van de Teammanagers.

Informatiebeveiliging draait niet alleen om het beschermen van gegevens; het is ook een belangrijke stimulator. Het stelt de RBG in staat om elektronische dienstverlening op een verantwoorde manier aan te bieden en ondersteunt nieuwe, innovatieve manieren van werken. De focus ligt op het veilig uitwisselen van informatie in alle vormen: digitaal, op papier en zelfs mondeling.

Beveiliging gaat daarbij verder dan techniek. Verantwoord en bewust gedrag van alle medewerkers is essentieel voor de informatieveiligheid. Informatiebeveiliging is een integraal onderdeel van de dagelijkse werkwijze binnen de RBG. Beveiligings- en Privacyaspecten worden structureel opgenomen in alle procesbeschrijvingen en werkinstructies, zodat veiligheid vanzelfsprekend onderdeel is van hoe we werken.

Beleidsproces
Het PDCA-cyclus, om het beveiligingsbeleid vast te stellen en hier uitvoering aan te geven, verloopt als volgt:

P. Formuleren van het informatiebeveiligingsbeleid en informatiebeveiligingsplan
D. Uitvoeren van de maatregelen
C. Jaarlijkse risicoanalyse – onderzoek waar welke risico's bestaan
A. Evaluatie en controle – onderdeel van de PDCA-cyclus



Evaluatie en controle

De controle op uitvoering van de vastgestelde beveiligingsmaatregelen wordt door de kwaliteitsmedewerkers uitgevoerd. De controles omvatten minimaal het volgende:

- Controle op naleving van het vastgestelde beleid en hieruit voortvloeiende richtlijnen en maatregelen;
- Controle op de implementatie en borging van maatregelen uit het beveiligingsplan;

Zij rapporteren hun bevindingen aan de CISO. Deze zal deze rapportage(s) aanvullen en rapporteren aan het MT.

De verantwoordelijkheid voor implementatie van de beveiligingsmaatregel ligt bij de Teammanagers. Zij dienen in hun reguliere PDCA-rapportages aandacht te besteden aan de voortgang van implementatie van maatregelen uit het beveiligingsplan.

BIV Classificatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt duidelijk welke maatregelen nodig zijn. Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid

Er zijn drie beschermingsniveaus van laag, midden en hoog. Het belang van informatie(systemen) voor de organisatie alsmede de privacy gevoeligheid van gegevens verschilt per systeem en gegeven. De Regionale Belasting Groep stelt normen op voor wat betreft beschikbaarheid, integriteit en vertrouwelijkheid. Deze normen liggen voor de RBG vast in het *proces-verbaal* ***"Gegevens classificatie"*** en worden vastgesteld door de Directie.

Meldplicht Incidenten

Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen.
Bij beveiligingsincidenten wordt de CISO altijd geïnformeerd.
Voor incidenten is een calamiteitenplan opgesteld. Hierin is een draaiboek opgenomen over hoe om te gaan en te handelen bij incidenten/calamiteiten. Hierin zijn onder andere opgenomen actuele contactlijsten en overzichten van leveranciers.

Alle beveiligingsincidenten en datalekken worden geregistreerd in het ISMS. Niet alleen het incident zelf wordt vastgelegd, ook de maatregelen die zijn genomen om de impact te beperken of weg te nemen. Deze informatie vormt de basis voor een evaluatie, zodat precies kan worden bepaald wat er is gebeurd en wat we daarvan kunnen leren.

Het doel van deze registratie helpt om bestaande beheersmaatregelen te verbeteren en nieuwe risico's eerder te herkennen. Zo groeit onze informatiebeveiliging continu mee met de praktijk en blijven de organisatie steeds beter beschermd

Voor het melden van een datalek heeft de RBG een *Protocol melding aan Autoriteit Persoonsgegevens opgesteld* (BIO norm 13.1.1.2).

Zodra de **Cyberbeveiligingswet CBW** van kracht is zullen beveiligingsincidenten worden gemeld bij het NSCS.

3. Vaststelling

Vastgesteld door het dagelijks bestuur van de Regionale Belasting Groep

Schiedam, 23 april 2026,

Directeur,

w.g.

J.F. Kooistra

Voorzitter,

w.g.

P. Ouwendijk

Referenties ter inzage bij de RBG

Documenten	Verantwoordelijk
Risicoschema en Data kwalificatie RBG	Directie
Matrix gegevens classificatie RBG	Directie
uitgangspunten autorisatie	Directie
Autorisatiematrix key2belastingen	Directie
Procesverbaal Gegevens classificatie	Directie
Protocol melding aan Autoriteit Persoonsgegevens	Directie
Wachtwoordbeleid	Directie
Gedragscode elektronisch verkeer V3	DB
Responsible disclosure	Directie
Gedragscode gebruik van bedrijfsmiddelen	Directie
Calamiteitenplan	