# Informatiebeveiligingsbeleid VRT

2023-2025

VEILIGHEIDSREGIO TWENTE

## Autorisatie

| OPSTELLERS: | BIJDRAGE IN DE WERKGROEP*: |
|---|---|
| Erik Meijerink | [Opmerkingen] |

## Versiegegevens

| VERSIE: | DATUM: | OMSCHRIJVING: |
|---|---|---|
| 1.0 | 31-10-2022 | [Samenvatting] |

Enschede, 24-10-2022
Versie 1.0

# Inhoudsopgave

# 1 Inleiding

De wereld om ons heen is veranderd. Digitalisering en werken in de Cloud is inmiddels niet meer weg te denken en gemeengoed geworden. Door onze, inmiddels, grote afhankelijkheid van informatiesystemen en snelle ontwikkelingen in de informatievoorzieningen zijn ook de bedreigingen groter geworden. Inmiddels is dit thema verweven met ons dagelijkse leven en processen van overheden, bedrijven en andere organisaties.

Een belangrijk onderdeel om hier goed uitvoering aan te kunnen geven is informatiebeveiliging. Informatiebeveiliging is het beschermen van gegevens tegen schadelijke aanvallen van buitenaf en binnenuit. Onder informatiebeveiliging verstaan we zowel het beveiligen van de hardware (servers, netwerken en computer) maar ook de data op al je apparaten (beschikbaarheid, integriteit en vertrouwelijkheid van je gegevens).

## 1.1 Aanleiding

De Veiligheidsregio Twente (VRT) beschikt over een vastgesteld overkoepelend informatiebeveiligingsbeleid en een uitvoeringsregeling (vastgesteld 2019). Echter is deze gedateerd en dringend toe aan een update.

Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor het Rijk, Gemeenten, Waterschappen en Provincies[1]. Hiermee ontstaat een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid.

De BIO verhoogt de informatieveiligheid bij alle bestuurslagen van de overheid. Eén gezamenlijke baseline voor alle overheidsorganisaties biedt vele voordelen. Het vergroot de informatieveiligheid en het vertrouwen, zorgt voor eenduidigheid en leidt bovendien tot kostenbesparing. Betere afstemming tussen (systemen van) overheidsorganisaties en partners. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (vastgelegd in de ISO). De BIO wordt op basis van nieuwe ISO-versies, door de NEN-organisatie gepubliceerd en geactualiseerd.

Dit beleidsdocument vormt het fundament voor het totale informatiebeveiligingsbeleid van de VRT.

[1] Veiligheidsregio wordt hier niet apart benoemd. Colleges van B&W van gemeenten die behoren tot een regio treffen een gemeenschappelijke regeling, waarbij een openbaar lichaam wordt ingesteld met de aanduiding Veiligheidsregio.

# 2 Doelstellingen en kaders

Het informatiebeveiligingsbeleid VRT heeft als doel:

*"Het waarborgen van de continuïteit van het bedrijfsproces en het minimaliseren van de schade door het voorkómen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen van deze incidenten".*

Het informatiebeveiligingsbeleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een norm en om de taken, bevoegdheden en verantwoordelijkheden in de VRT te beleggen. Het kader wordt uitgewerkt in een set beheersmaatregelen. De VRT toetst of:

a) Er gehandeld wordt volgens afgesproken beleid;
b) Of de beheersmaatregelen werkbaar zijn in de praktijk.

Uit bovenstaande doelstelling komen de volgende elementen en randvoorwaarden voort die verdere invulling behoeven om het doel te kunnen realiseren:

- Normen: de basis voor de inrichting van het VRT-informatiebeveiligingsbeleid is dit beleidsdocument, waarvoor ISO 27001 als inspiratie dient. Formele certificering volgens ISO 27001 wordt voor VRT niet als noodzakelijk gezien, inrichting van een goed Information Security Management System (ISMS) echter wel – dit beleid is daarvoor de basis;
- Maatregelen: maatregelen worden genomen op basis van best practices, waarbij de op ISO 27002 gebaseerde Baseline Informatiebeveiliging Overheid als uitgangspunt dient;
- Uitgangspunten en organisatie van informatiebeveiliging zijn vastgelegd in dit beleidsstuk en worden gedragen door het bestuur, en afgeleid daarvan, door de gehele VRT. De criteria 's genoemd in de BIO, worden in separate beleidstukken uitgewerkt;
- Een daadkrachtig proces: duidelijke keuzes in maatregelen, actieve controle op beleidsmaatregelen en de uitvoering daarvan;
- Compliance: het beleid biedt de basis om te voldoen aan wettelijke normen.

## 2.1 Doelgroep

Het informatiebeveiligingsbeleid van de VRT valt onder de verantwoordelijkheid van het bestuur en leidinggevenden. Het beleid is van toepassing op alle medewerkers (ambtelijk, beroeps, vrijwilligers), gasten, bezoekers en (externe) relaties, maar ook ketenpartners in de crisisorganisatie. Kortom, iedereen die – intern dan wel extern – op enige manier te maken heeft met (aspecten van) het bedrijfsproces van de VRT, 24 uur per dag, 7 dagen per week, 365 dagen per jaar.

## 2.2 Scope en afbakening

Zoals ook al in de aanleiding beschreven is, vormt dit kader de grondslag voor het totale informatiebeveiligingsbeleid van de VRT. In onderliggend stuk worden op hoofdlijnen de (beleids-)kaders van het informatiebeveiligingsbeleid beschreven. Hierbij kan gedacht worden aan o.a. de focus en richting van het beleid maar ook welke onderwerpen hieronder vallen. Alle onderdelen die binnen het informatiebeveiligingsbeleid vallen worden uitgewerkt in separate documenten (voorbeelden zijn: Toegangsbeleid, Wachtwoordbeleid, Clear/clean desk, Telewerken etc. Al deze documenten samen vormen het informatiebeveiligingsbeleid voor de VRT.

## 2.3 Taken VRT versus Platformtaken

De wettelijke taken van de VRT zijn vastgelegd in de wet Veiligheidsregio's en omvatten risico- en crisisbeheersing en brandweerzorg. De geldende wet- en regelgeving die voor de werkzaamheden van de VRT van toepassing zijn, als het gaat om de genoemde onderwerpen, zijn de uitgangspunten voor het informatiebeveiligingsbeleid van de VRT.

Daarnaast geeft de VRT ook uitvoering aan platformtaken. Denk hierbij aan het platform Integrale Veiligheidszorg (IVZ) en het Zorg- en Veiligheidshuis Twente. Deze platformen werken in basis meer samen met andere ketenpartners (medisch en strafrechtelijk) waardoor hier een afwijkende (en mogelijk verdergaande) wijze van informatiebeveiliging aan ten grondslag ligt.

De VRT hanteert het principe dat voor de bepaling van de scope en reikwijdte van het informatieveiligheidsbeleid de (wettelijke) taken en informatieveiligheidsrisico's van de VRT het vertrekpunt vormen. Voor platform-taken geldt dat ze van daaruit zo goed mogelijk worden ondersteund. Er worden geen organisatie brede aanvullende of extra maatregelen genomen die specifiek zijn voor (de informatieveiligheidsrisico's van) deze taken.

## 2.4 Versiebeheer

Dit informatiebeveiligingsbeleid geldt voor de periode van 2023 – 2025. Het beleid is toegespitst op de feitelijke situatie binnen de organisatie en zal hierdoor in principe na drie jaar geëvalueerd en indien nodig bijgesteld worden. Als zich in de tussentijd significante wijzigingen binnen de wet- en regelgeving of onvoorziene omstandigheden voordoen, kan besloten worden om de termijn van drie jaar eerder af te breken en het beleid waar nodig bij te stellen.

# 3 Wet- en regelgeving

In Nederland is verschillende wet- en regelgeving beschikbaar op het gebied van informatieveiligheid en bescherming van persoonsgegevens. In dit hoofdstuk wordt de belangrijkste wet- en regelgeving waaraan de VRT moet voldoen beschreven.

## 3.1 BIO

Binnen de overheid is er één gezamenlijk basisnormenkader ontwikkeld voor informatiebeveiliging: de BIO. VRT is als overheidsinstelling gebonden aan dit normenkader. De BIO is een gezamenlijk kader voor informatiebeveiliging (I-Beveiliging) binnen alle overheidslagen waaronder ook de veiligheidsregio's vallen. Eén basisniveau voor informatiebeveiliging dat gebaseerd is op de internationaal erkende en actuele ISO-systematiek. Concreet bestaat de BIO uit een set van 114 beheersmaatregelen, die te clusteren zijn naar een 16-tal criteria 's. Globaal bestaat de BIO uit:

1. Strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene informatiebeveiligingsbeleid en beveiligingsbeleid;
2. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
3. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan leidinggevenden;
4. De gemeenschappelijke betrouwbaarheidseisen en normen die op de VRT van toepassing zijn;
5. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;
6. De bevordering van het beveiligingsbewustzijn.

De 16 criteria 's zijn hieronder schematisch weergegeven:

## 3.2 AVG

Daarnaast is de Algemene Verordening Gegevensbescherming (AVG) van toepassing binnen de VRT. Overheden, bedrijfsleven en verenigingen moeten hieraan voldoen. Door deze wetgeving krijgen mensen meer zelfbeschikking over hun privacy rechten. Organisaties moeten hun systemen hierop inrichten. De Verordening is de opvolger van de Wet bescherming persoonsgegevens in Nederland. Het doel van de Verordening is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie ('EU'). Doel is het faciliteren van vrij verkeer, mogelijk gemaakt door veiligheid. In het kort bestaat de AVG uit:

1. Spelregels voor de Verwerking van persoonsgegevens;
2. Bescherming van rechten van betrokkenen;
3. Duiding rolverdeling tussen verwerkingsverantwoordelijke en verwerker;
4. Verantwoordingsplicht;
5. Invulling van specifieke rollen: Functionaris Gegevensbescherming (FG), Chief Information Security Officer (CISO) en Privacy Officer (PO). In het kader van de AVG zijn deze (extra) rollen binnen de VRT opgenomen, zij dragen zorg voor de uitvoering van de AVG.

# 4 Uitgangspunten

Als basis voor onderliggend beleid zijn een aantal uitgangspunten vastgesteld. Deze uitgangspunten hebben betrekking op zowel het doel, de inrichting als de uitvoering.

1. **VRT voldoet aan alle van toepassing zijnde wet- en regelgeving, nu en in de toekomst**
   Uitgangspunt is dat de VRT voldoet aan alle van toepassing zijnde wet- en regelgeving en zich voorbereidt om aan wijzigingen in wetgeving tijdig te voldoen. Landelijke en Europese ontwikkelingen worden gemonitord en waar nodig geïmplementeerd.

2. **Platformen, die vallen onder de VRT, conformeren zich aan het informatiebeveiligingsbeleid van de VRT.**
   De VRT kent verschillende samenwerkingsverbanden. Voorbeelden hiervan zijn: platform IVZ en Zorg- en Veiligheidshuis Twente. De eisen van het informatiebeveiligingsbeleid zijn gebaseerd op de reguliere taken van de VRT. In basis conformeren de platformen zich aan bij het informatiebeveiligingsbeleid van de VRT.

3. **VRT voldoet aan de landelijke minimumgrens volwassenheidsniveau BIO**
   De BIO kent vijf volwassenheidsniveau ‘s (1 t/m 5). De volwassenheidsniveau ’s van de BIO worden gebruikt om te groeien in volwassenheid door het feitelijk verbeteren van informatiebeveiliging. Om aan de BIO te voldoen moet minimaal aan landelijke minimumgrens niveau 3 worden voldaan, maar ook een aantal eisen op niveau 4 en één op niveau 5. Een voorbeeld van een minimumgrens is ‘Personeelsbeleid’ (verantwoordelijkheden voor het beschermen en beveiligen van bedrijfsinformatie) en een voorbeeld op niveau 4 is ‘IB-organisatie’ (taken, bevoegdheden en rollen op informatiebeveiliging vaststellen, toewijzen etc).

4. **VRT streeft naar een adequaat beveiligingsniveau waarbij een goede balans tussen functionaliteit en beveiligingsmaatregelen wordt gewaarborgd.**
   Niet alle maatregelen die op het gebied van informatiebeveiliging genomen moeten worden bevorderen de gebruiksvriendelijkheid voor de medewerkers. Het is echter is wel van belang dat de beveiliging dusdanig is dat de continuïteit van de bedrijfsprocessen gewaarborgd kan worden. Hiervoor worden risicobeoordelingen uitgevoerd. Bij tegengestelde belangen of als een goede balans niet kan worden gevonden hanteren we het principe: beveiliging voor functionaliteit.

5. **Iedere medewerker is zich bewust van het belang van informatiebeveiliging**
   Medewerkers binnen de VRT worden bewust gemaakt en getraind om actief bij te dragen aan de informatiebeveiliging. Ze zijn op de hoogte van de verantwoordelijkheden (bewustzijn) - en de geldende procedures, voorschriften en gedragscodes die gelden binnen de VRT.

6. **Binnen de VRT is informatiebeveiliging ieders verantwoordelijkheid**
   Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging volledig uit te sluiten. De mens zelf creëert de grootste risico’s. Elke medewerker, externen, gasten en/of leveranciers is verantwoordelijk voor en levert een bijdrage aan het informatiebeveiligingsbeleid.

7. **VRT maakt gebruikt van standaarden en best practices**
   Alle overheidsinstanties moeten voldoen aan onder meer de BIO en doen ervaring op tijdens de implementatie en uitvoering van de BIO. Binnen de VRT kijken we naar best practices op het gebied van informatiebeveiligingsmaatregelen en vinden we niet zelf ‘het wiel’ opnieuw uit.

8. **VRT streeft naar Goede communicatie over informatieveiligheid en privacy**
   Het succes van een goede informatiebeveiliging staat of valt met een goed communicatiebeleid. Informatiebeveiliging is dynamisch en zal altijd in ontwikkeling blijven. Het is belangrijk om de gebruikers van de systemen en voorzieningen mee te nemen (op hoofdlijnen) in de ontwikkelingen en aan te geven waarom er wijzigingen noodzakelijk zijn. Dit zorgt voor meer draagvlak en begrip. Uitgangspunt is daarom dat over dit onderwerp regelmatig, helder en transparant wordt gecommuniceerd.

# 5 Governance

Het goed en verantwoord sturing geven aan de VRT wordt aangeduid met governance. Een goede governance zorgt er voor dat alle belanghebbenden de rechten en plichten kennen. De governance van de VRT is belegd is de volgende rollen en/of functies belegd. De taken, verantwoordelijkheden en bevoegdheden zijn als volgt belegd:

**Voorzitter VRT**
De voorzitter van de Veiligheidsregio is bestuurlijk verantwoordelijk voor het informatiebeveiligingsbeleid. Het Algemeen Bestuur stelt het beleidskader vast.

**Portefeuillehouder informatieveiligheid**
De secretaris van de VRT is met de invoering van de AVG in 2018 aangewezen als portefeuillehouder informatieveiligheid. Informatieveiligheid en informatiebeveiliging hebben veel raakvlakken. Om deze reden is gekozen om beide onderwerpen te beleggen bij deze functionaris. De secretaris van de VRT legt verantwoording af aan het Algemeen Bestuur.

**Sectorhoofd S&O**
Het sectorhoofd S&O is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid van de VRT. Hieronder wordt verstaan: het inzichtelijk maken van de risico's, het opstellen van kaders, het monitoren van de naleving en het doen van verbetervoorstellen om het beveiligingsniveau continue te verbeteren. Het sectorhoofd rapporteert integraal over informatiebeveiliging aan de veiligheidsdirectie.

**Chief Information Security Officer**
De Chief Information Security Officer (CISO) is verantwoordelijk voor de strategische en tactische toepassing en naleving van het informatiebeveiligingsbeleid. Bewaakt de naleving ten aanzien van relevante wet- en regelgeving en adviseert over informatiebeveiligingsmaatregelen en bewaakt de consistentie van de maatregelen.

**Functionaris Gegevensbescherming**
De functionaris gegevensbescherming (FG) is verantwoordelijk voor het toezicht op en de naleving van de AVG.

**Privacy Officer**
De privacy officer is verantwoordelijk voor het vormgeven en implementeren van het gegevensbeschermingsbeleid binnen de VRT. Daarnaast is de privacy officer belast met het in kaart brengen van risico's door bijvoorbeeld een Protection Impact Assessment (PIA) uit te voeren.

**Teamleider OIV**
De teamleider OIV is verantwoordelijk voor de uitvoering van de operationele beveiligingsmaatregelen in het kader van het informatiebeveiligingsbeleid. Denk bijvoorbeeld aan de inrichting en het beheer van de systemen.

**Leidinggevenden VRT**
De leidinggevenden binnen de VRT zijn verantwoordelijk voor de aansturing en uitvoering van de operationele beveiligingsmaatregelen in het kader van het informatiebeveiligingsbeleid richting medewerkers.

**Medewerkers / externen (gasten & leveranciers)**
Informatiebeveiligingsbeleid begint bij het individu. Dit houdt in dat iedere medewerker verantwoordelijk is voor hun eigen informatiebeveiliging. Medewerkers dienen de door de VRT voorgeschreven beveiligingsmiddelen en informatiebeveiligingsmaatregelen te gebruiken en te volgen. Ook zijn ze zich bewust van relevante wet- en regelgeving en signaleren van (potentiële) beveiligincidenten.

**Ketenpartners in crisisorganisatie**
De VRT faciliteert operationele beveiligingsmaatregelen waar ketenpartners tijdens crisis gebruik van maken. De medewerker is eindverantwoordelijk voor informatiebeveiliging. De medewerker dient zich aan de door de VRT voorgeschreven beveiligingsmiddelen en informatiebeveiligingsmaatregelen te conformeren.

## 5.1 Overlegstructuur

Onder verantwoordelijkheid en onder het voorzitterschap van de CISO vindt periodiek een overleg informatieveiligheid plaats om de stand van zaken, uitvoering van beleid en onderhoud van de BIO te monitoren. Dit overleg wordt gevormd door: CISO, sectorhoofd S&O, Teamleider IOV, FG ondersteund voor een beleidsadviseur. Afhankelijk van specifieke thema's worden inhoudsdeskundigen aan het overleg toegevoegd.

Daarnaast staat het onderwerp BIO structureel op de agenda van het Bedrijfsvoering Overleg (BVO) van de VRT. Uitvoeringsafspraken en -procedures, zoals Toegangsbeleid, Wachtwoordbeleid, Clear/clean desk, Telewerken etc., worden in dit gremium vastgesteld.