Informatiebeveiligingsbeleid VRT

Strategisch beleid B-01.01

VEILIGHEIDSREGIO TWENTE

Versie	Wijzigingen
1.0	Initiële versie

Autorisatie

Beheerder document: CISO

Inhoudsopgave

1 Inleiding

De rol van informatieprocessen en informatievoorziening in onze wereld is groot en veranderd voortdurend. Digitalisering en werken in de cloud is inmiddels niet meer weg te denken en gemeengoed geworden. Door onze grote afhankelijkheid van informatiesystemen en snelle ontwikkelingen in
informatievoorzieningen zijn ook de bedreigingen op dat thema groter geworden. Inmiddels zijn die bedreigingen verweven met ons dagelijkse leven en in informatieprocessen van en met onze stakeholders zoals overheden, bedrijven en andere organisaties.
Een belangrijk aspect om hier goed mee om te gaan is een op risico gebaseerde informatiebeveiliging.

1.1 Wat is informatiebeveiling?

Informatiebeveiliging wordt als volgt gedefinieerd: "*Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen*."
Informatiebeveiliging omvat dus een *samenhangend stelsel* van maatregelen. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd. Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit wordt bereikt door een zorgvuldige afweging van kosten en baten in relatie tot het te beheersen risico.

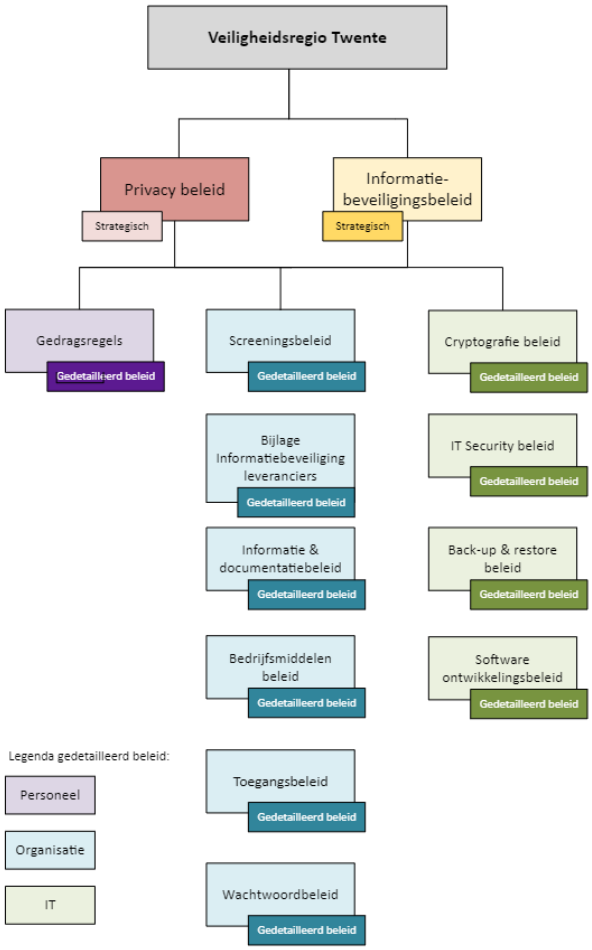
Zoals in de voorgaande definitie is verwoord, richt informatiebeveiliging zich op de volgende drie aspecten van de informatievoorziening:

- *Beschikbaarheid*, de informatie moet op de gewenste momenten beschikbaar zijn;
- *Integriteit*, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- *Vertrouwelijkheid*, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

1.2 Toelichting document

Dit informatiebeveiligingsbeleid is een document op hoofdlijn, waarin de beleidsverklaring van de directie en de uitgangspunten voor informatiebeveiliging zijn opgenomen. De actualiteit en de geschiktheid van het informatiebeveiligingsbeleid wordt jaarlijks beoordeeld of zodra zich belangrijke veranderingen voordoen.

Daarnaast zijn er nog onderwerp specifieke beleidsdocumenten. Zie hiervoor de onderstaande structuur van beleidsdocumenten voor informatiebeveiliging binnen VRT:



Figuur 1: Structuur beleidsdocumenten

1.3 Doelgroep

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

1.4 Communicatie

Interne belanghebbenden

- De directie communiceert periodiek de strekking van informatieveiligheidsbeleid binnen onze organisatie.
- Het team Mens en Organisatie is verantwoordelijk voor het informeren van nieuwe medewerkers en contractanten over informatieveiligheid binnen de Veiligheidsregio Twente.
- De Veiligheidsregio Twente zorgt voor de beschikbaarheid van alle beleidsdocumenten.
- De medewerker moet alle relevante beleid hebben gezien en begrepen.

Ketenpartners in crisisorganisatie

- De Veiligheidsregio Twente faciliteert operationele beveiligingsmaatregelen waar ketenpartners tijdens crisis gebruik van maken. De medewerker is verantwoordelijk voor informatiebeveiliging. De medewerker dient zich aan de door de Veiligheidsregio Twente voorgeschreven beveiligingsmiddelen en informatiebeveiligingsmaatregelen te conformeren.

Externe belanghebbenden

- Via onze website bieden wij belangstellenden de mogelijkheid om ons informatiebeveiligingsbeleid op te vragen.

2 Beleidsverklaring en continue verbeteren

2.1 Beleidsverklaring

Het belangrijkste doel van het informatiebeveiligingsbeleid is het definiëren van de uitgangspunten van en de verantwoordelijkheden voor informatiebeveiliging in overeenstemming met contractuele eisen en toepasselijke wet- en regelgeving.

Iedereen binnen de Veiligheidsregio Twente is bij het uitvoeren van werkzaamheden afhankelijk van informatie.
De directie van de Veiligheidsregio Twente vindt informatie dan ook een belangrijk bedrijfsmiddel, dat goed moet worden beschermd. Daarom zijn er beleidsregels opgesteld, procedures beschreven en beheersmaatregelen geïmplementeerd. Daarnaast vindt de directie het belangrijk dat iedereen de beleidsregels, procedures en beheersmaatregelen naleeft en uitvoert. Directie en management hebben hierin een voorbeeldfunctie.

Als het gaat om informatieveiligheid, dan zorgt de Veiligheidsregio Twente ervoor dat medewerkers:

- goed zijn geïnstrueerd over en richtlijnen hebben gekregen van hun rollen en verantwoordelijkheden voordat zij toegang krijgen tot vertrouwelijke informatie;
- gemotiveerd zijn om de beleidsregels voor informatiebeveiliging na te leven;
- worden geïnformeerd over en betrokken bij actuele zaken rondom informatieveiligheid;
- zwakke plekken en incidenten zonder uitstel of belemmering melden.

2.2 Managementsysteem voor informatiebeveiliging

Het managementsysteem voor informatiebeveiliging wordt meestal afgekort met ISMS en dat staat voor het Engelse, Information Security Management Systeem.

- Het managementsysteem voor informatiebeveiliging is ingericht als proces.
- De beheersmaatregelen voor informatiebeveiliging zijn geïmplementeerd in het ISMS op basis van ISO27001 Annex A en de Baseline Informatiebeveiliging Overheid (BIO).
- Het ISMS wordt periodiek gecontroleerd binnen de reikwijdte die is vastgesteld in de contextbeschrijving.
- Het ISMS sluit aan op de bestaande Planning & Control-cyclus van onze organisatie.

2.3 Continue verbeteren

Het ISMS-proces wordt bestuurd via de plan-do-check-act-cyclus. Met behulp van deze cyclus wordt continue verbetering nagestreefd.

- Risicoanalyse dient als een belangrijke basis voor continue verbetering van de beveiliging van informatie binnen de Veiligheidsregio Twente.
- Het gewenste risiconiveau wordt vastgesteld door middel van periodieke risicobeoordeling.
- Nieuwe beheersmaatregelen worden geïmplementeerd waar nodig en bestaande beheersmaatregelen worden aangescherpt.
- Het afbakenen of verkleinen van beheersmaatregelen die niet langer relevant zijn, is ook mogelijk om overmatige controle te voorkomen.

3 Uitgangspunten voor informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen onze organisatie worden de volgende **uitgangspunten** gehanteerd:

1. De Veiligheidsregio Twente voldoet aan de landelijke minimumgrens volwassenheidsniveau 3 van de BIO.
2. De Veiligheidsregio Twente voldoet aan van toepassing zijnde wet- en regelgeving en vereiste normenkaders. In dit verband worden onder andere genoemd: Wet Veiligheidsregio's, Algemene Verordening Gegevensbescherming (AVG) en Baseline Informatiebeveiliging Overheid.
3. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Verantwoordelijkheden voor informatiebeveiliging zijn toegewezen en vastgelegd voor alle teams binnen de Veiligheidsregio Twente.
4. Wanneer (onderdelen) van de Veiligheidsregio Twente samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.
5. De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van de Veiligheidsregio Twente zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
6. Bij de aanname, tijdens het dienstverband, functiewisseling en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
7. De Veiligheidsregio Twente voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren.
8. De Veiligheidsregio Twente beschikt over gedragsregels voor het gebruik van informatie en informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
9. Bij overtreding van de gedragsregels voor informatiebeveiliging en/of relevante wettelijke bepalingen kan het management gebruik maken van de disciplinaire procedure en een sanctie zoals non-actiefstelling, disciplinaire straffen of beëindiging van het dienstverband opleggen.
10. De Veiligheidsregio Twente heeft maatregelen getroffen voor de fysieke beveiliging van mensen en middelen.
11. De Veiligheidsregio Twente heeft maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen.
12. De VRT heeft maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
13. Bij informatiesystemen wordt in alle fasen van de levenscyclus van het informatiesysteem nadrukkelijk aandacht besteed aan informatiebeveiliging.
14. De Veiligheidsregio Twente heeft adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) zoveel mogelijk is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
15. De eigenaren van de maatregelen toetsen periodiek de naleving van de getroffen maatregelen en rapporteren de resultaten aan de CISO (1e lijn controle).
16. Als onderdeel van het informatiebeveiligingsproces wordt binnen de Veiligheidsregio Twente door interne (2e lijn controle) en externe partijen (3e lijn controle) toegezien op de naleving van het informatiebeveiligingsbeleid.
17. De Veiligheidsregio Twente beschikt over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.

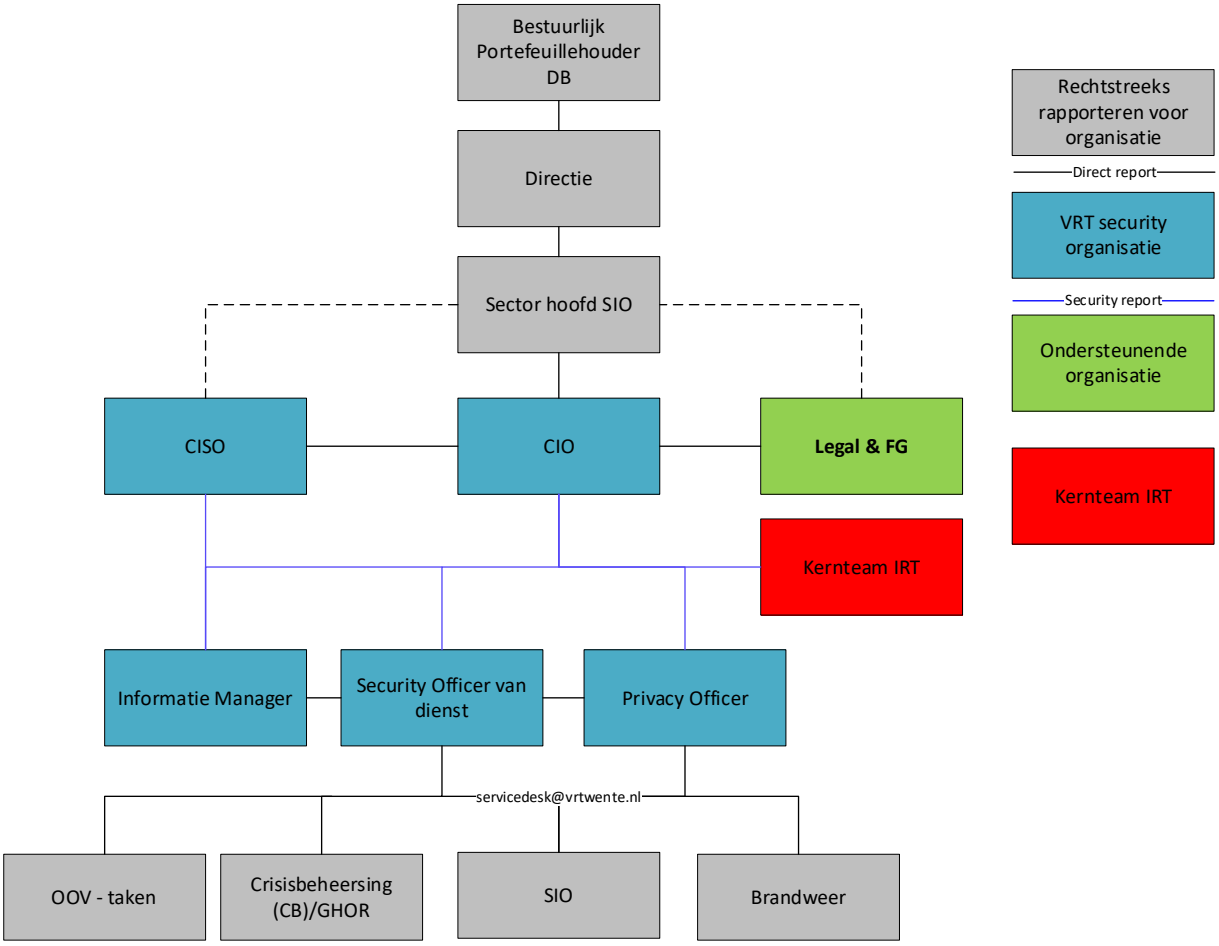
Een aantal van deze uitgangspunten zijn uitgewerkt in informatiebeveiligingsdoelstellingen. Deze doelstellingen zijn tevens gebaseerd op de context van de organisatie.

4 Middelen en verantwoordelijkheden

4.1 Middelen

De directie van de Veiligheidsregio Twente zal ervoor zorgen dat voldoende middelen en medewerkers beschikbaar worden gesteld voor het onderhoud van het managementsysteem voor informatiebeveiliging en voor het bereiken van de informatiebeveiligingsdoelstellingen.

4.2 Security & Privacy organisatie



Figuur 2: Security & Privacy organisatie

4.3 Rollen en verantwoordelijkheden

Directie

De directie van de Veiligheidsregio Twente zal regelmatig het belang van de beveiliging van informatie en naleving van relevante beleidsrichtlijnen benadrukken. Zij zijn tevens verantwoordelijk voor het vaststellen van de noodzakelijke rollen, verantwoordelijkheden en bevoegdheden van de beveiliging van informatie. Daarnaast zal de directie actief deelnemen aan evaluatieactiviteiten die worden uitgevoerd om de algehele effectiviteit van het ISMS te bepalen en om de beveiligingsdoelstellingen af te stemmen op de strategische richting van de organisatie.

Sectorhoofden en teamleiders
Van sectorhoofden en teamleiders wordt verwacht dat zij:

- De gedragscode voor informatiebeveiliging actief uitdragen en erop toe zien dat dit wordt nageleefd.
- Informatiebeveiliging als onderwerp meenemen in de gesprekscyclus met hun teamleden.
- Processen voor informatiebeveiliging implementeren binnen hun team en erop toe zien dat dit wordt nageleefd.
- Wijzigingen in informatieprocessen – en systemen (zoals aanpassingen of vernieuwing van hard- en software) altijd uitvoeren in samenspraak met de IT-afdeling.

Medewerkers
Van medewerkers wordt verwacht dat zij actief informeren naar en/ of kennis hebben van:

- Beleidsregels, processen en procedures die belangrijk en relevant zijn voor de functie.
- Wet- en regelgeving (AVG).
- Gedragscode voor informatiebeveiliging.

CISO
De CISO is verantwoordelijk voor de informatiebeveiliging binnen de Veiligheidsregio Twente. Het organiseren van informatiebeveiliging omvat:

- Het onderhouden, en indien nodig, wijzigen of uitbreiden van het ISMS, met inbegrip van privacy gerelateerde onderwerpen in samenspraak met de FG en PO;
- Monitoren en evalueren van de prestaties van het ISMS en het betrekken van directie, management en medewerkers bij deze prestaties.
- Coördineren van interne- en externe audits voor informatiebeveiliging.
- Geven van praktisch advies over informatiebeveiliging.
- Organiseren van activiteiten om het bewustzijn van informatiebeveiliging binnen de Veiligheidsregio Twente te bevorderen in samenspraak met de PO.
- Bij aanschaf van nieuwe softwareapplicaties en diensten, wordt de CISO betrokken om informatiebeveiliging in kaart te brengen.
- Zorgen voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming.

CIO
De CIO is verantwoordelijk voor:

- Leidinggeven aan het personeel van het team informatievoorziening
- Strategieën bepalen en doelen formuleren met betrekking tot ICT infrastructuur
- Beheren en optimaal doen presteren van bestaande ICT infrastructuur.
- Leidinggeven aan de CIO office organisatie met daarin de CISO, PO en Informatie Manager.

Informatie manager
De informatiemanager is verantwoordelijk voor:

- Informatiecoördinatie: Zorgen voor een efficiënte stroom van informatie tussen verschillende teams en organisaties binnen de Veiligheidsregio.
- Beeldvorming: Het verzamelen, analyseren en verspreiden van informatie om een duidelijk en actueel beeld van informatiebehoefte te creëren.
- Ondersteuning van besluitvorming: Het leveren van accurate en tijdige informatie aan besluitvormers om hen te ondersteunen bij het nemen van weloverwogen beslissingen rondom informatievoorziening.
- Procesbeheer: Het sturen en coördineren van de informatievoorziening, inclusief het inwinnen, vastleggen en gebruiken van informatie.
- Beleid en strategie: Ontwikkelen en implementeren van informatiebeleid en strategieën die aansluiten bij de lange termijn doelstellingen van de Veiligheidsregio.
- Projectmanagement: Leidinggeven aan projecten die gericht zijn op het verbeteren van de informatievoorziening en het implementeren van nieuwe technologieën en systemen.

Security Officer van dienst
De Security Officer van dienst zorgt voor de uitvoerende en monitoring taken van informatiebeveiliging binnen de Veiligheidsregio Twente.

Onder de uitvoerende taken van informatiebeveiliging vallen

- Snelle reactie op beveiligingsincidenten om de impact te minimaliseren en verdere schade te voorkomen.

Security team
Tot de taken van het Security team behoren:

- Analyse van gedetecteerde incidenten om de aard en omvang van de dreiging te begrijpen;
- Opgeschaalde incidenten en niet opgeschaalde;
- Het leveren van input aan verbeterprojecten die de beveiliging bevorderen;
- Communicatie met externe belanghebbenden.

Privacy Officer
De taken van de Privacy Officer zijn beschreven in het Privacy beleid.

Functionaris gegevensbescherming
De taken van de Functionaris gegevensbescherming zijn beschreven in het Privacy beleid.

4.4 Overlegstructuur

Binnen de VRT zijn voor het onderhoud van het ISMS en de informatieveiligheid de volgende overleggen ingevoerd:

OVERLEG	DEELNEMERS	FREQUENTIE	VERSLAGLEGGING
Informatiebeveiliging overleg.	CISO (vz) en Sectorhoofd SIO	Kwartaal	Actie- en besluitenlijst
Voortgangsoverleg Informatiebeveiliging.	CISO (vz), Security Officer van Dienst, FG, Privacy Officer, Informatiemanager en CIO	Maandelijks	Actie- en besluitenlijst