Strategisch Informatiebeveiligings- & privacybeleid 2025-2028

Samenwerken aan veiligheid.

VEILIGHEIDS REGIO BRABANT-NOORD

Uitgave en redactie
Veiligheidsregio Brabant-Noord, 3-7-2025

Versie:	Datum:	Door:	Activiteit:
1.0	3-7-2025	MTVR	Vastgesteld

Meer informatie
Adviseur Informatiebeveiliging (CISO)
Functionaris Gegevensbescherming
Privacy Adviseur

In Veiligheidsregio Brabant-Noord wonen, werken en recreëren ruim 670.000 inwoners in 11 gemeenten. Binnen de Veiligheidsregio werken brandweer, GHOR, politie, meldkamer en gemeenten samen op het gebied van brandweerzorg, crisisbeheersing, geneeskundige hulpverlening bij ongevallen & rampen en rampenbestrijding.

2 Samenwerken aan veiligheid.

Inhoudsopgave

1. Inleiding

1.1 Algemeen

Informatiebeveiliging is voor alle veiligheidsregio's een actueel thema en binnen Veiligheidsregio Brabant-Noord (hierna: VRBN) een relevant onderdeel van het beleidsplan 2024 - 2027[1].

Nieuwe digitale ontwikkelingen volgen elkaar in rap tempo op en informatie speelt een steeds belangrijkere rol in de organisatie. De digitale weerbaarheid wordt steeds belangrijker in het adequaat uitoefenen van ons vak. Dit maakt het noodzakelijk voor VRBN om alert te zijn en te blijven. Een veilige en betrouwbare informatievoorziening is hierbij cruciaal.

VRBN heeft te maken met externe bedreigingen en interne risico's doordat steeds meer gegevensstromen[2] worden gekoppeld. Keuzes tussen transparantie en openheid van informatie enerzijds en beveiliging van vertrouwelijke informatie anderzijds vragen om zorgvuldige afweging.

Dit document bevat het strategische deel van het informatiebeveiligings- en privacybeleid. Het beschrijft op hoofdlijnen welke uitgangspunten VRBN hanteert voor een goede bescherming van de informatie en hoe de organisatie hiervoor is ingericht.

1.2 Aanleiding

VRBN beschikt over een vastgesteld informatiebeveiligings- en privacybeleid (beide vastgesteld 2018). Dit moet worden bijgewerkt omdat het beleid is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Per 1 januari 2019 is de BIG vervangen door de BIO (Baseline Informatiebeveiliging Overheid). Naast de BIO wordt tevens de ISO27001 als standaard gehanteerd voor informatiebeveiliging. VRBN streeft naar een ISO27001 certificering[3] omdat verschillende processen de status 'vitaal' krijgen, wat vraagt om strikte informatiebeveiliging. Door deze certificering kunnen we aantonen dat we de informatiebeveiliging op orde hebben. De BIO is niet auditbaar, waardoor het moeilijk is om aantoonbaar te maken dat we volledig aan de eisen voldoen.

[1] Beleidsplan 2024 -2027
[2] Met gegevensstromen wordt bedoeld de verplaatsing en verwerking van gegevens binnen een systeem of netwerk, van verzameling tot opslag, gebruik, en uiteindelijke verwijdering.
[3] Vastgesteld door MTVR op 10-02-2025

2. Doelstelling en Kaders

2.1 Doel informatiebeveiligings- en privacybeleid

Het informatiebeveiligings- en privacybeleid van VRBN heeft als doel het waarborgen van de beschikbaarheid, integriteit, vertrouwelijkheid van informatie, informatiemiddelen en bedrijfsprocessen, door middel van preventieve, detectieve, repressieve en correctieve maatregelen. Dit draagt bij aan het minimaliseren van risico's, het voorkomen van schade, beveiligingsincidenten en datalekken, en het waarborgen van de continuïteit van de informatievoorziening die de organisatie levert aan burgers, ketenpartners en interne afdelingen.

De doelen van het informatiebeveiligings- en privacy beleid van VRBN zijn de volgende:

- *Kader:* het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging en privacy te toetsen aan vastgestelde eisen die door het MT zijn gesteld.
- *Normen:* de basis voor de inrichting van het security-management is de ISO27001 en de Baseline Informatiebeveiliging Overheid (BIO). De basis voor de inrichting van privacy management is de Algemene Verordening Gegevensbescherming (AVG) in combinatie met de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).
- *Daadkrachtig:* het beleid dient als basis voor duidelijke keuzes in maatregelen, actieve controle op beleidsregels en de uitvoering daarvan.
- *Helderheid:* het beleid biedt duidelijkheid, is ondubbelzinnig en is voor iedereen binnen VRBN te begrijpen en toe te passen.
- Continuïteit informatievoorziening: informatie zowel digitaal als fysiek dient te allen tijde beschikbaar te zijn voor de continuïteit en beschikbaarheid van onze operationele (vitale) werkprocessen.

Dit doen we door te werken aan de volgende subdoelstellingen:

Slim samenwerken met techniek, mensen en ketenpartners door de juiste software en hardware te kiezen, die veilige en efficiënte samenwerking mogelijk maakt.

Kennis en innovatie op het gebied van informatiebeveiliging en privacy richten zich op het ontwikkelen van technologieën en processen om data te beschermen tegen dreigingen. Door voortdurende innovatie kan VRBN de beveiliging verbeteren en voldoen aan de eisen van privacywetgeving en gegevensbescherming.

Veerkracht en wendbaarheid op het gebied van informatiebeveiliging en privacy zorgen ervoor dat de organisatie snel kan reageren op dreigingen en incidenten zonder de veiligheid van gegevens in gevaar te brengen. Met robuuste beveiliging en flexibele processen blijft de organisatie beschermd en kan VRBN zich snel aanpassen aan nieuwe risico's en wetgeving.

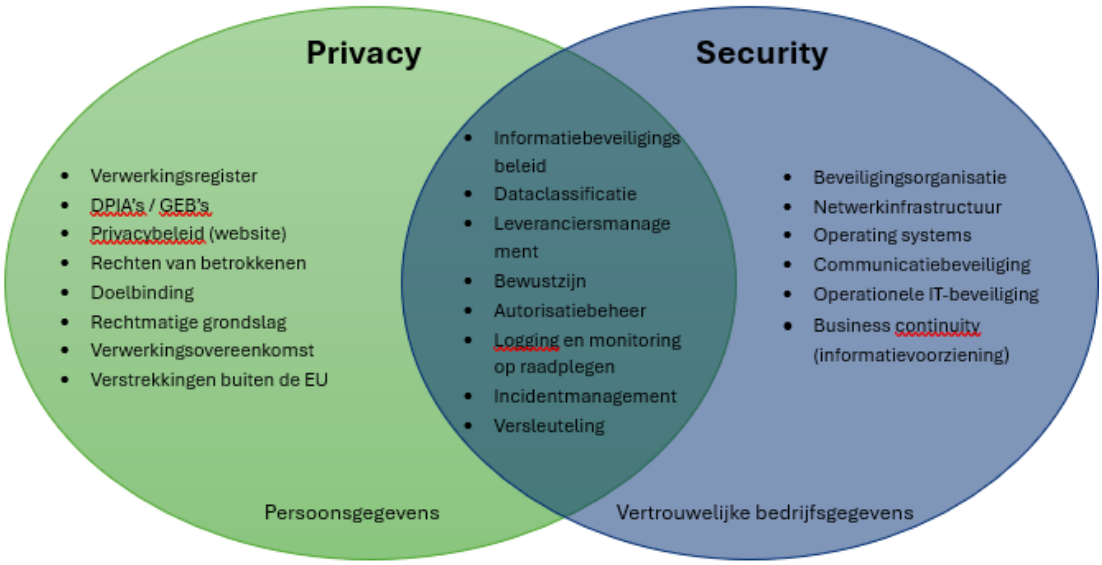
Mens en werk in balans. Informatiebeveiliging en privacy worden ingericht om de werkzaamheden te ondersteunen zonder obstakels te creëren. Het is belangrijk dat medewerkers veilig kunnen werken met informatie zonder onnodige belemmeringen. Zo blijft de balans tussen mens en werk behouden, met het juiste beveiligingsniveau dat efficiënt en gebruiksvriendelijk is.

2.2 Doelgroep

Het informatiebeveiligings- en privacybeleid is van toepassing op alle medewerkers (beroeps, vrijwilligers, externe medewerkers, tijdelijke inhuur en stagiaires) van VRBN.
Wanneer er informatie door VRBN wordt gedeeld met derden worden hierover afspraken gemaakt en vastgelegd in het contract, convenant of verwerkingsovereenkomst.

2.3 Scope

Zoals in de aanleiding beschreven is, vormt dit beleid de grondslag voor het totale informatiebeveiligings- en privacybeleid van VRBN. In onderliggend stuk worden op hoofdlijnen de (beleids-)kaders van het informatiebeveiligings- en privacybeleid beschreven. De overeenkomsten en verschillen tussen informatiebeveiliging (security) en privacy zijn als volgt.



Dit beleid geldt voor alle informatie, zowel fysiek als digitaal, binnen VRBN en dekt al haar informatiebeveiliging- en privacyeisen. Het is van toepassing op alle bedrijfsprocessen en iedereen die met deze informatie werkt (medewerkers, ketenpartners, bezoekers, externe relaties zoals bijvoorbeeld inhuur/outsourcing). Het gaat daarbij om de bescherming van hardware, software, locaties, fysieke documentatie en mensen.

2.4 Kwaliteitsmanagement

Vanuit kwaliteitsmanagement is er aandacht voor het continu leren over informatiebeveiliging en privacy. Wij streven naar consistentie, actualiteit, kwaliteit en betrouwbaarheid in al onze processen. Om dit te waarborgen, hanteren wij een kwaliteitsmanagementsysteem gebaseerd op de PDCA-cyclus (Plan-Do-Check-Act).

Continu leren staat centraal. Daarmee zorgen we ervoor dat het informatiebeveiligings- en privacybeleid blijft aansluiten bij de actualiteit (denk aan nieuwe ontwikkelingen of verandering wet- en regelgeving).

3. Definitie informatiebeveiliging

3.1 De definitie die VRBN hanteert

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen, gericht op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de informatievoorziening.

3.2 Beschikbaarheid, Integriteit en Vertrouwelijkheid

De criteria om applicaties te categoriseren zijn de BIV-classificaties: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Deze classificatie is standaard voor informatieveiligheid en is gebaseerd op de classificeringcriteria van de ISO27001.

- **Beschikbaarheid** gaat over (bedrijfs)continuïteit. De applicatie en data (digitaal en/of fysiek) moeten beschikbaar zijn voor het werkproces. Maatregelen beperken dat de applicatie of fysieke opgeslagen data niet beschikbaar is.
- **Integriteit** gaat over de kwaliteit in de vorm van juistheid en volledigheid van de data in de applicaties. Het werkproces moet juiste, volledige en actuele informatie leveren. Maatregelen beperken dat het werkproces onjuiste, onvolledige en/of niet actuele informatie oplevert.
- **Vertrouwelijkheid** gaat over de mate waarin er de mogelijkheid is applicaties en data in te zien of te delen met derden. Door het juist beheren kan een gedefinieerde groep kennisnemen van data in de applicatie. Maatregelen beperken dat informatie in handen komt van ongeautoriseerde derden.

De applicatiecategorie is afhankelijk van alle drie de classificaties. Afhankelijk van de categorie worden de uitgangspunten en richtlijnen toegepast en wordt waar nodig maatregelen genomen.

3.3 Mens, techniek en proces

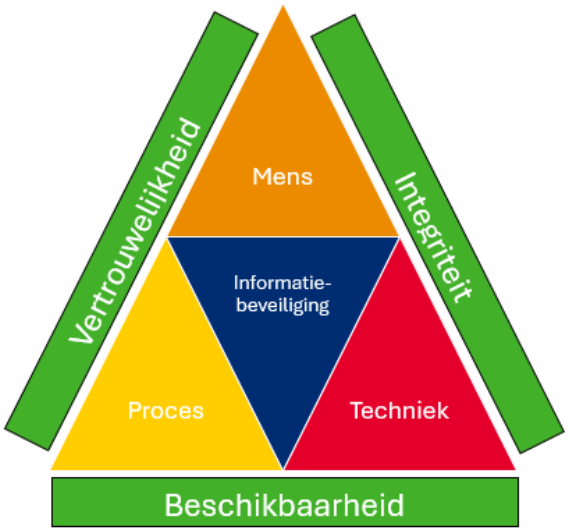
Naast de bovengenoemde betrouwbaarheidsaspecten spelen ook de mens, techniek en proces een cruciale rol in informatiebeveiliging. Deze elementen vormen samen de basis voor informatiebeveiliging.

- **Mens**:
  - Bewustwording en training van medewerkers over beveiligingsrisico's.
  - Beleid en gedragsregels die zorgen voor veilig gebruik van informatie.
  - Verantwoordelijkheid bij alle medewerkers voor het naleven van beveiligingsmaatregelen.

- **Proces**:
  - Duidelijke richtlijnen en procedures voor het omgaan met vertrouwelijke informatie.
  - Periodieke audits en risicobeoordelingen om kwetsbaarheden te identificeren.
  - Incidentresponsplannen voor het snel en effectief reageren op beveiligingsincidenten.

- **Techniek**:
    - Implementatie van technologische oplossingen zoals firewalls, encryptie, segmentatie en antivirussoftware.
    - Toegangscontrole en authenticatie om ongeautoriseerde toegang te voorkomen.
    - Continue monitoring en updates van systemen om nieuwe bedreigingen te kunnen afweren.

Een effectieve informatiebeveiliging vraagt om een balans en samenwerking tussen deze drie pijlers, waarbij de mens centraal staat in het handhaven van de juiste processen en het effectief inzetten van technische middelen.



3.4 Classificatie

Classificatie is essentieel voor informatiebeveiliging en privacy omdat het helpt om een proces, applicatie en gegevens te categoriseren op basis van gevoeligheid van de gegevens en belang van de gegevens voor de organisatie. Classificatie is een cruciale stap in het waarborgen van de integriteit en vertrouwelijkheid van informatie. Classificatie:

Stelt de organisatie in staat om gerichte beveiligingsmaatregelen te implementeren die passen bij de risiconiveaus van verschillende classificaties en gegevens.

- Maakt duidelijk welke informatie extra bescherming vereist. Zo verlagen we de kans op datalekken en ongeoorloofde toegang.
- Helpt bij de naleving van wet- en regelgeving, zoals de ISO27001, BIO en AVG, door te waarborgen dat gevoelige gegevens juist worden beheerd.
- Vergemakkelijkt ook de training en bewustwording van medewerkers over hoe zij met verschillende soorten gegevens moeten omgaan.
- Helpt bij een effectieve incidentrespons door snel te identificeren welke gegevens betrokken zijn bij een beveiligingsincident.

3.4.1 Type classificaties

- Classificatie van processen:
    - Dit betreft het indelen van bedrijfsprocessen op basis van hun belangrijkheid en impact op de organisatie.
    - De classificatie helpt bij het prioriteren van beveiligingsmaatregelen en middelen.

- Classificatie van applicaties
    - Applicaties ondersteunen processen en hebben verschillende beveiligingsbehoeften afhankelijk van hun functie en de gevoeligheid van de verwerkte gegevens.
    - Door applicaties te classificeren op basis van hun rol in kritische processen, kan de organisatie bepalen welke applicaties extra bescherming vereisen. Niet te verwarren met categoriseren[4] van applicaties.

- Classificatie van data:
    - Gegevens worden vaak geclassificeerd op basis van hun gevoeligheid en belang voor de organisatie (bijvoorbeeld openbaar, intern, vertrouwelijk).
    - De classificatie van data beïnvloedt de benodigde BIV-aspecten. Vertrouwelijke data vereisen striktere maatregelen om integriteit en vertrouwelijkheid te waarborgen.

[4] Zie applicatiebeleid hoofdstuk 6.

4. Definitie privacy

4.1 De definitie die VRBN hanteert

Privacy is van toepassing op alle verwerkingen van persoonsgegevens van de betrokkenen. Persoonsgegevens zijn alle gegevens die te herleiden zijn, direct of indirect, tot een natuurlijk persoon. Voor alle verwerkingen moet een duidelijk doel zijn vastgesteld waaruit blijkt dat het gebruik van de persoonsgegevens niet onredelijk is en in verhouding staat tot het beoogde resultaat. Om transparantie te waarborgen moet het doel en de verantwoording vastgelegd zijn en inzichtelijk kunnen zijn voor de personen van wie de gegevens verwerkt worden, de betrokkenen. Zodra de persoonsgegevens niet meer nodig zijn voor het beschreven doel, moeten we zorgen dat de gegevens verwijderd worden.

4.2 Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. In onze organisatie is de rol van verantwoordelijke belegd bij leidinggevende. De verantwoordelijke beslist of er persoonsgegevens verwerkt worden, en zo ja:

- Om welke verwerking(en) het gaat;
- Welke persoonsgegevens de organisatie hierbij verwerkt;
- Voor welk doel de organisatie dit doet;
- Op welke manier de organisatie dit doet;
- De verwerking wordt toegevoegd aan het verwerkingsregister;
- Ziet erop toe dat de PDCA-cyclus wordt gehanteerd.

4.3 Verwerkingsregister

Alle verwerkingen van persoonsgegevens worden vastgelegd in het verwerkingsregister. Het register wordt gefaciliteerd door de Functionaris Gegevensbescherming en de Privacy Adviseur en wordt gevuld door de verwerkingsverantwoordelijken.

4.4 Rechtmatige grondslag

Voor alle verwerkingen van persoonsgegevens dient vooraf een grondslag te worden bepaald.

- U heeft toestemming van de persoon om wie het gaat.
- Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
- Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
- Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen van betrokkenen.
- Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang uit te voeren / openbaar gezag uit te oefenen.
- Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

4.5 Privacy by Design, Privacy by Default

Bij privacy by design gaat het om aandacht voor gegevensbescherming in de ontwerpfase van een product of dienst. Privacy by default houdt in dat de standaardinstellingen zo privacy-

vriendelijk mogelijk moeten zijn. Beide uitgangspunten zijn verplicht bij het verwerken van persoonsgegevens.

4.6 Risicoanalyse

Bij elk ontwerp van informatiesystemen of andere vorm van gegevensverwerking zal minimaal en doelmatig gebruik van persoonsgegevens het uitgangspunt zijn. Voor nieuwe systemen en grote aanpassingen, waaruit blijkt dat er sprake is van een verhoogd privacy risico, wordt er onder verantwoordelijkheid van de verwerkingsverantwoordelijke in samenwerking met de FG een impact analyse op de informatiebescherming (DPIA) uitgevoerd. Indien de gegevens op enig moment buiten de EU worden verwerkt, zal de opdrachtgever in samenwerking met de FG eveneens een transfer impact analyse uitvoeren (DTIA).

4.7 Verwerkingsovereenkomst

Het uitbesteden van de verwerking mag niet ten koste gaan van de afspraken die met de betrokkene(n) van de persoonsgegevens zijn gemaakt. Dat is precies waar een verwerkersovereenkomst voor is. Hiermee regelt de verwerkersverantwoordelijke dat die derde partij zorgvuldig met de persoonsgegevens omspringt en zich bovendien houdt aan de afspraken die met de betrokkenen daarover gemaakt zijn. VRBN hanteert hiervoor zijn eigen verwerkersovereenkomst.

4.8 Privacyverklaring

Bij de eerste verzameling van persoonsgegevens wordt aan (toekomstige) relaties, (toekomstige) medewerkers en website bezoekers (de betrokkenen) kenbaar gemaakt dat gegevens worden verzameld. Hierbij wordt een privacyverklaring gehanteerd waarbij het doel van de verwerking duidelijk vermeld wordt en de rechten die betrokkenen hebben ten aanzien van de verzamelde gegevens uiteengezet worden.

4.9 Persoonsgegevens werknemers

Werknemers hebben verschillende rechten met betrekking tot persoonsgegevens. Werknemers hebben het recht om te weten welke gegevens worden verwerkt, om onjuiste of onvolledige gegevens te laten corrigeren en te laten verwijderen (tenzij ze wettelijk verplicht zijn ze te bewaren) en recht op inzage.

5. Randvoorwaarden en uitgangspunten

Randvoorwaarden

De randvoorwaarden zijn:

- De implementatie, uitvoering en handhaving van informatiebeveiliging en privacy valt onder verantwoordelijkheid van het lijnmanagement en wordt gedragen door het MTVR van VRBN.
- Risicomanagement is uitgangspunt bij informatiebeveiliging en privacy.
- Kennis en expertise zijn cruciaal voor informatiebeveiliging en privacy en moet worden geborgd.
- Informatiebeveiliging en privacy vereist een integrale aanpak, zowel binnen VRBN en voor onze ketenpartners.

5.1 Uitgangspunten

De uitgangspunten van het informatiebeveiligings- en privacybeleid zijn:

- Informatiebeveiliging en werkbaarheid worden altijd zorgvuldig afgewogen, zodat de bescherming van informatie nooit ten koste gaat van de continuïteit van vitale bedrijfsprocessen.
- Informatiebeveiliging en gegevensbescherming bij VRBN vindt plaats conform geldende wet- en regelgeving.
- Regels en verantwoordelijkheden voor de uitvoering van het beleid worden door de CISO, FG en Privacy Adviseur opgesteld en door het MTVR vastgesteld in separate uitvoeringsdocumenten en richtlijnen.
- Alle informatiebronnen en -systemen waarvoor VRBN verantwoordelijk is hebben een applicatieeigenaar die gezamenlijk met de CISO en/of FG de classificatie bepaalt. De uitvoering van informatiebeveiliging en privacy binnen de informatiebronnen en -systemen is een verantwoordelijkheid van de eigenaren. De directeur VRBN is eindverantwoordelijk voor de informatiebeveiliging en privacy.
- Voldoen aan informatiebeveiliging en privacy is een continu verbeterproces. De methode ‘Plan, do, check en act’ vormt de basis van het managementsysteem van informatiebeveiliging en privacy.
- De door VRBN gehanteerde eisen op het gebied van informatiebeveiliging en privacy maken deel uit van afspraken met ketenpartners en leveranciers.
- Kennis en bewustzijn van informatiebeveiliging en privacy en omgaan met vertrouwelijke informatie en persoonsgegevens binnen de organisatie wordt actief door de CISO, FG en Privacy Adviseur bevorderd en geborgd (awareness).
- Iedere medewerker, zowel vast als tijdelijk, beroeps of vrijwilliger, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken
- VRBN stelt de benodigde mensen en middelen beschikbaar om invulling te kunnen geven aan informatiebeveiliging en privacy volgens de wijze zoals gesteld in dit beleid.
- Afwijking van beleid vindt plaats conform het “pas toe of leg uit”[5] principe en worden beargumenteerd vastgelegd.

[5] Volgens het 'pas toe of leg uit'-principe worden de bepalingen in het informatiebeveiligings- en privacybeleid nageleefd door deze toe te passen of uit te leggen waarom van de betreffende bepalingen wordt afgeweken.

6. Wet- en regelgeving

In Nederland geldt wet- en regelgeving op het gebied van informatieveiligheid en bescherming van persoonsgegevens. In dit hoofdstuk wordt de belangrijkste wet- en regelgeving waaraan VRBN moet voldoen of zich aan heeft geconformeerd beschreven.

6.1 Algemene Verordening Gegevensbescherming (AVG)

Overheden, bedrijfsleven en verenigingen moeten voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Door deze wetgeving krijgen mensen meer zelfbeschikking over hun persoonsgegevens en kunnen zij hun privacyrechten uitoefenen. Organisaties moeten hun systemen en processen hierop inrichten. Het doel van de AVG is om twee belangen te waarborgen: de bescherming van natuurlijke personen aangaande de verwerking van hun persoonsgegevens en het faciliteren van het vrije verkeer van persoonsgegevens binnen de Europese Unie ('EU').

6.2 ISO27001

ISO 27001 is een norm voor informatiebeveiliging die helpt bij het beschermen van gevoelige informatie en het minimaliseren van de risico's van beveiligingsincidenten. De ISO 27001 bevat in totaal 114 normen. Deze normen omvatten alle aspecten van informatiebeveiliging, zoals risicobeheer, beveiligingsbeleid en naleving van wet- en regelgeving.

De normen zijn onder te verdelen in verschillende thema's zoals in bijlage 2 is weergegeven:

6.3 Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is gebaseerd op de ISO27001 norm. Op specifieke normen geeft de BIO een nadere invulling in de vorm van overheidsmaatregelen. Binnen VRBN wordt de ISO27001 norm gehanteerd en zal waar nodig aanvullende BIO maatregelen worden geïmplementeerd.

6.4 Open standaarden[6]

Alle (semi-) overheidsorganisaties hebben de verplichting om de open standaarden op de 'Pas toe of leg uit'-lijst toe te passen. Forum Standaardisatie adviseert de publieke sector over het gebruik van ICT-standaarden. Als computersystemen gegevens uitwisselen, dan moeten zij de afspraken en vaste processen hanteren.

6.5 NIS2[7]

De NIS2-richtlijn biedt een uitzondering voor overheidsinstanties die hoofdzakelijk activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving. Dit betekent bijvoorbeeld dat o.a. de veiligheidsregio's zijn uitgesloten van de NIS2-richtlijn. Veiligheidsregio's dienen wel een gelijk niveau van weerbaarheid te hebben.

[6] Zie: 'Pas toe leg uit' standaarden (verplicht) | Forum Standaardisatie
[7] Zie: NIS2-richtlijn NIS2-richtlijn - Digitale Overheid

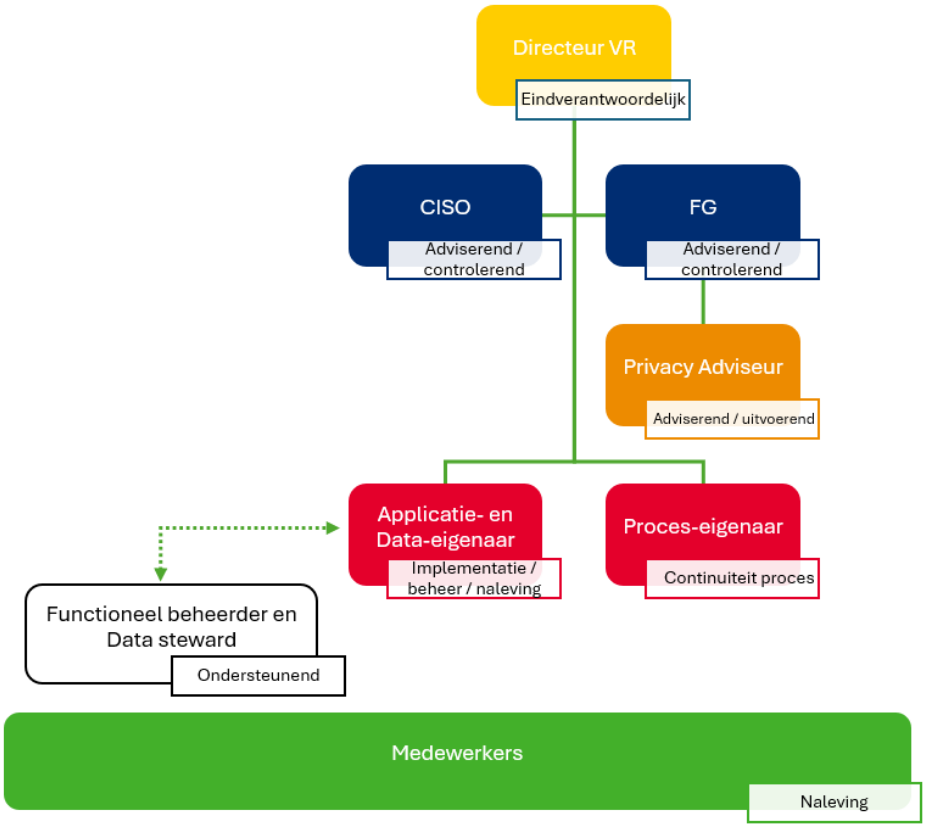
7. Organisatie van informatiebeveiliging en privacy

7.1 Organisatie

Door het inrichten van een informatiebeveiligings- en privacy organisatie zorgt VRBN voor passende aandacht en sturing. Iedereen die werkt binnen de organisatie heeft een verantwoordelijkheid. Dit wordt op vier niveaus ingericht.

- De directeur is te allen tijde eindverantwoordelijk voor de informatiebeveiliging en privacy van de organisatie.
- De CISO, FG en Privacy Adviseur ondersteunen, adviseren, coördineren en bewaken of dit beleid wordt nageleefd.
- De proceseigenaren, applicatie-eigenaren en data eigenaren hebben een cruciale rol bij het uitvoeren van dit informatiebeveiligings- en privacybeleid. Zo maken zij een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de organisatie heeft, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan wordt dit beleid voor informatiebeveiliging opgezet, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
    - De functioneel beheerders en data steward zijn ondersteunend aan de proces-, applicatie- en dataeigenaren.
- Alle medewerkers binnen de organisatie zijn verantwoordelijk voor het naleven van interne richtlijnen en procedures rondom informatiebeveiliging en privacy.

[8]



[8] Nader toelichting over de rollen applicatie- ,data- en proceseigenaar, functioneel beheerder en Data steward is terug te vinden in het document Data Governance (in ontwikkeling).

7.2 Taken en verantwoordelijkheden

Voor informatiebeveiliging en privacy worden binnen VRBN de volgende taken en verantwoordelijkheden onderkend:

Functie:	Verantwoordelijkheid Rol
Algemeen Directeur	Is eindverantwoordelijk voor de Informatiebeveiliging en privacy van de organisatie.
Sectorhoofd en teamleider	Is verantwoordelijk voor het actief uitdragen en controle op naleving van informatiebeveiliging en privacy binnen de organisatie. Dit houdt in: – Dat de benodigde capaciteit en middelen beschikbaar zijn voor de uitvoering van het beleid informatiebeveiliging en privacy. – Dat het belang van doeltreffende informatiebeveiliging gecommuniceerd wordt naar de organisatie. – De medewerkers van de afdeling in staat stellen het beleid uit te voeren door duidelijke instructies en het laten volgen van bewustzijnstrainingen. – De medewerkers van de afdeling in staat stellen om afwijkingen op het beleid en incidenten te kunnen identificeren en melden. – Zorgdragen dat informatiebeveiliging en privacy zijn geborgd bij de inkoop van diensten en producten; – De teamleiders zijn aangewezen als verwerkingsverantwoordelijken, ze beslissen of er persoonsgegevens verwerkt worden en met welk doel.
Proces[9]-, applicatie- en dataeigenaar[10]	Is verantwoordelijk voor Informatiebeveiliging en borging van privacy binnen zijn/haar proces, applicatie of data. De verantwoordelijkheden als eigenaar behelzen onder andere: – Dat de eisen uit het beleid informatiebeveiliging en privacy zijn geïmplementeerd binnen de processen en applicaties van de organisatie. – Risico's identificeren en indien nodig te mitigeren. – Eventuele restrisico's voorleggen aan CISO en/of FG. – Bekend zijn met het beleid voor informatiebeveiliging en privacy en deze specifiek implementeren binnen het proces of applicatie. – Zorgdragen dat verbeteringen worden doorgevoerd waar afwijkingen zijn geconstateerd. – Betrokken zijn bij of verzorgen van de training en begeleiding van de medewerkers op het gebied van het informatiesysteem/de applicatie. – Beheren en onderhouden van de bij het informatiesysteem/de applicatie behorende gebruikersdocumentatie.
CISO	De CISO vervult een adviserende en controlerende rol binnen de organisatie. Dit houdt in:

[9] VRBN heeft momenteel nog geen proceseigenaren vastgesteld. Dit betreft een toekomstige ontwikkeling.
[10] VRBN heeft momenteel nog geen dataeigenaren vastgesteld. Dit betreft een toekomstige ontwikkeling en onderdeel van de datastrategie.

	– Coördineren en bewaken van het managementproces van informatiebeveiliging volgens de PDCA-cyclus. – Ontwikkelen van, samen met andere afdelingen, operationele richtlijnen, procedures en beleidsmaatregelen voor informatiebeveiliging. – Coördineren van de uitvoering van het informatiebeveiligings- en privacybeleid en zorgen voor naleving binnen de organisatie. – Adviseren aan de organisatie met betrekking tot informatiebeveiliging. – Organisatie breed verhogen van het bewustzijn rond informatiebeveiliging. – Initiëren van audits om de werking van informatiebeveiligingsmaatregelen te controleren en waar nodig verbeteringen door te voeren. – Rapporteren en informeren naar MTVR inzake de staat van informatiebeveiliging binnen de organisatie.
FG	De FG houdt onafhankelijk toezicht op de naleving van de AVG door de organisatie. Daarnaast geeft de FG gevraagd en ongevraagd advies over onderwerpen en kwesties die de privacyrechten raken van de medewerkers en overige betrokkenen.
Privacy Adviseur	– Stimuleren van het bewustzijn rondom privacy in de organisaties. – Uitvoeren van risicoanalyses op verwerkingsprocessen. – Actueel houden van het verwerkingsregister. – Afhandelen van datalekken. – Adviseren over complexe privacyvraagstukken
Medewerkers	Alle medewerkers (beroeps, vrijwilligers, externe medewerkers, tijdelijke inhuur en stagiaires): – Zijn zich bewust van het beleid en de onderliggende richtlijnen en procedures en handelen daarnaar. – Zorgen dat gegevens en informatiesystemen voldoende beschermd zijn tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht. – Melding te maken van vermeende beveiligingsincidenten en datalekken.

7.3 Naleving

Samen werken aan veiligheid
Naleving van informatiebeveiliging en privacy is een gezamenlijke verantwoordelijkheid. Het is niet alleen een kwestie van regels en richtlijnen maar ook gedrag. Door samen te werken en bewust om te gaan met informatie, werken we samen aan digitale veiligheid.

8. Information Security Management System (ISMS)

8.1 ISMS

De moderne kijk op Informatieveiligheid vereist dat een organisatie een Information Security Management System (ISMS) heeft ingericht. Het doel van ISMS is het stelselmatig en ook procesmatig sturen, ontwikkelen, verbeteren en borgen van de informatieveiligheid. Een ISMS omvat een PDCA (Plan, Do, Check, Act) gerichte verbetercyclus voor informatieveiligheid. Een vast onderdeel van die verbetercyclus is de uitvoering van ISO27001 risicoanalyses. Daarmee worden specifieke interne en externe organisatierisico's rondom informatiebeveiliging in kaart gebracht en worden passende beveiligingsmaatregelen toegewezen. Op deze manier verlagen we de risico's. De CISO, FG, proces- applicatie- en dataeigenaren maken hierbij continu afwegingen en keuzes of informatie in bestaande en nieuwe processen juist beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

8.2 PDCA cyclus

Informatiebeveiliging en Privacy is een continu verbeterproces. 'Plan, do, check, act' vormen samen het management systeem van informatiebeveiliging en Privacy.

- **Plan**: De cyclus start met informatiebeveiligings- en privacybeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de BIO, AVG of ISO27001. Deze zijn uitgewerkt in regels en maatregelen voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Dit beleid wordt jaarlijkse bijgewerkt.
- **Do**: De uitgangspunten zijn de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
- **Check**: Evalueren van de effectiviteit van de geïmplementeerde maatregelen en processen. In deze fase worden de resultaten van de acties die in de "Do"-fase zijn uitgevoerd gecontroleerd en vergeleken met de vooraf vastgestelde doelstellingen en normen. Dit gebeurt door middel van audits, controles, risicobeoordelingen en monitoring van systemen om te bepalen of er zwakke punten, non-conformiteiten of verbeterpunten zijn.
    - Externe controle betreft een controle die wordt uitgevoerd buiten het primaire proces door bijvoorbeeld een externe auditor in het kader van een certificering. Bevindingen, aanpak en risico-classificatie worden gerapporteerd aan MT-VRBN.
- **Act**: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning. De interne controlerapportage conform PDCA wordt verwerkt (en vastgelegd conform) in de interne controlerapportages VRBN breed, gerapporteerd door concerncontrol. Afwijkingen wordt gerapporteerd aan het Dagelijks Bestuur van VRBN.

Bijlage 1: Afkortingen en toelichtingen

AVG	De afkorting AVG staat voor **Algemene Verordening Gegevensbescherming**. Dit is dé privacywetgeving, die sinds mei 2018 in de hele Europese Unie (EU) geldt. Goed om te weten: de AVG is ook bekend onder de Engelse naam: General Data Protection Regulation (GDPR).
BIO	Per 1 januari 2020 is de **Baseline Informatiebeveiliging Overheid** (BIO) van kracht. BIO is het normenkader voor informatiebeveiliging binnen de gehele overheid, op basis van actuele ISO-normatiek. Voorheen hadden de verschillende bestuurslagen (gemeenten, rijk, waterschappen en provincies) elk hun eigen baseline. Voor gemeenten was dat de BIG: Baseline Informatiebeveiliging Gemeenten.
BIV	Een BIV-classificatie of BIV-indeling is een indeling die binnen de informatiebeveiliging wordt gehanteerd, waarbij de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt aangegeven. BIV staat voor Beschikbaarheid, Integriteit, Vertrouwelijkheid.
CISO	CISO staat voor Chief Information Security Officer (CISO) en is in een organisatie verantwoordelijk voor de informatiebeveiliging en daarmee ook het aanspreekpunt over dit onderwerp.
DPIA	Data Protection Impact Assessment is een analyse van een verwerking om te bepalen welke gevolgen die verwerking heeft voor de bescherming van persoonsgegevens. Een DPIA kan uitwijzen dat er teveel gegevens verwerkt worden, waardoor de gegevensbescherming van betrokkenen wordt geschaad. Of dat de betrokkene zijn rechten niet effectief kan uitvoeren, waardoor hij niet kan weten wat er precies gebeurd met zijn persoonsgegevens.
FG	De functionaris gegevensbescherming (FG) houdt binnen een organisatie toezicht op de toepassing en naleving van de privacywetgeving. Zij hebben een onafhankelijke functie. Voor sommige organisaties is het verplicht een FG aan te stellen en die aan te melden bij de Autoriteit Persoonsgegevens (AP).
ISMS	ISMS staat voor Information Security Management System en is een managementsysteem voor informatiebeveiliging.
ISO27001	International Standardization Organization (ISO). ISO27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. De norm beschrijft hoe je

	procesmatig met het beveiligen van informatie kunt omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen de organisatie zeker te stellen.
ISO-normen	De Baseline Informatiebeveiliging Overheid (**BIO**) is geheel gestructureerd volgens **NEN-ISO/IEC 27001:2017** en NEN-ISO/IEC 27002:2017. De BIO beschrijft de invulling van deze normen voor de overheid, maar vervangt deze niet.
MTVR	Managementteam van Veiligheidsregio Brabant-Noord.
PDCA-cyclus	De PDCA-cyclus (**Plan-Do-Check-Act**) is een methode waarmee je stap voor stap je werk, prestaties en organisatie beter kunt maken om zo continu te verbeteren.
VRBN	Afkoring voor Veiligheidsregio Brabant-Noord.

Bijlage 2: Thema uitwerking ISO27001 / BIO

IB-beleid is passend effectief en cyclisch

IB-organisatie is formeel ingesteld en gepositioneerd

Informatiebeveiliging is verankerd in **personeelsbeleid**

Werkomgevingen (fysiek/online) zijn passend beveiligd

Toegang tot de ICT-infrastructuur is logisch beveiligd

Systeembeheer borgt wijzigingen en bewaakt prestaties

IB-incidenten worden vastgelegd om van te leren

ICT wordt beschermd tegen **kwetsbaarheden en aanvallen**

Netwerken en Informatiestromen worden bewaakt

Testen/ontwikkelen kent procedures en security by design

Wetten/contracten worden aantoonbaar nageleefd

Cryptografie wordt in beleid geborgd en passend uitgevoerd

Back-up / redundantie / uitwijk is onderdeel van BCM

De lifecycle **van alle apparatuur en data** is geregistreerd

In **leveranciersbeheer** zijn risicoafwegingen doorslaggevend

Periodiek vinden **audits en beoordelingen** plaats adhv ISMS

Bijlage 3: Thema uitwerking AVG

Samenwerken aan veiligheid.

VEILIGHEIDS REGIO BRABANT-NOORD