

Oplegnotitie Besluitvormend

Onderwerp	Informatieveiligheidsbeleid 2023-2026
Ter behandeling in de vergadering van	het Algemeen Bestuur
Status	Openbaar
Portefeuillehouder	De heer de Vries
Auteur	De heer Kleinhuis
Bijlagen	1.Informatieveiligheidsbeleid 2023-2026 VRF
Vergaderdatum	15-12-2022
Agendapunt	9
Betrokken afdeling/ medewerkers (functioneel)	
OR/GO	Kies een item.

Conceptbesluit	-Vaststellen van het Informatieveiligheidsbeleid 2023-2026
Inleiding	<p>De wereldwijde digitalisering en de technologische ontwikkelingen maken het leven makkelijker en zijn goed voor onze welvaart. Ze vormen ook een risico. Het beveiligen van informatie is een steeds ingewikkelder probleem. Spionage, beïnvloeding, sabotage en diefstal hebben grootschalig hun intrede gedaan in het digitale domein. En ook VRF is voor de uitvoering van haar taken steeds afhankelijker geworden van een goede informatievoorziening. Eigenlijk is informatie en informatievoorziening niet meer weg te denken in het kader van bijvoorbeeld grootschalige vaccinatieprogramma's, de uitvoering van brandweertaken of het met ketenpartners uitvoering geven aan crisisbeheersing.</p> <p>Het thema 'Kansen en bedreigingen van de informatie- en data-gestuurde maatschappij' is dan ook één van de vier thema's van de Strategische Agenda Veiligheidsberaad. Binnen dit thema werkt het Veiligheidsberaad aan o.a. een bestuurlijk programma voor het onderwerp Digitale ontwricting. Uitval van digitale systemen, kunnen een versturende of zelfs ontwrictende uitwerking hebben in de maatschappij, ook in de fysieke omgeving. Daarnaast kan een digitale verstoring het optreden van hulpdiensten belemmeren. Het Veiligheidsberaad stelt zich hierbij ook de vraag in hoeverre de veiligheidsregio's zijn voorbereid op deze risico's.</p> <p>Het Veiligheidsberaad heeft derhalve in juni 2021 aan de besturen van de Veiligheidsregio's gevraagd deel te nemen in het zg, 'Versnellingsplan informatieveiligheid' en zo zorg te dragen voor een afdoende veiligheidsniveau van haar informatievoorziening.</p>

	<p>Hiervoor dienen de Veiligheidsregio's eind 2022 te voldoen aan de Baseline Informatieveiligheid Overheid (BIO), het binnen de overheid afgesproken kader voor informatieveiligheid.</p> <p>Om naar dit afgesproken niveau toe te werken is bij VRF een project gestart en een plan gemaakt op basis waarvan wordt toegewerkt naar het gaan voldoen aan de basisnormen van de BIO en aanvullend hierop ook te voldoen aan de normen uit de NEN (7510 e.a.) voor het gezondheidsbedrijf binnen VRF. In dit kader dient er ook een beleid voor informatieveiligheid te zijn vastgesteld waarin de belangrijkste uitgangspunten en verantwoordelijkheden zijn geformuleerd. Dit nieuwe beleid ligt nu voor ter vaststelling en vervangt daarmee het beleid dat eerder in 2012 in het Dagelijks Bestuur is vastgesteld.</p> <p>De grote verandering in het denken van nu op gebied van informatieveiligheid ten opzichte van 2012 is dat informatieveiligheid naast het voldoen aan normen, steeds meer gezien wordt als een managementproces. Risicomanagement staat hierin centraal. De inrichting van dit risicomanagement en het bijbehorende managementproces voor informatieveiligheid zal komende periode nog de nodige aandacht vragen binnen VRF.</p> <p>In het Veiligheidsberaad wordt verder nog gesproken over een eventuele tweede fase van het 'Versnellingsplan informatieveiligheid'. De tweede fase omvat mogelijk het opzetten van een goede monitoring (SOC) en incident respons (CERT) voor veiligheidsregio's. Dit is enerzijds een verplicht onderdeel vanuit de BIO, anderzijds wordt de noodzaak ervan ook gelinkt aan de mogelijke/aanstaande 'vitaal' verklaring van (processen) van Veiligheidsregio's.</p>
<p>Beoogd effect</p>	<p>Het verbeteren en borgen van de beschikbaarheid en kwaliteit van de dienstverlening en taken van VRF door aandacht te geven aan informatieveiligheid. Tevens het voldoen aan wet- en regelgeving en aan de verwachtingen van onze stakeholders.</p>
<p>Argumenten</p>	<p>De beschikbaarheid, integriteit en exclusiviteit van informatie en informatievoorziening zijn randvoorwaardelijk voor VRF om haar taken goed en zeker te kunnen vervullen. De klanten, partners en ook onze bestuurders verwachten daarbij dat wij goed en veilig met onze (of hun) informatie en informatievoorziening omgaan.</p>
<p>Kantttekeningen/risico's</p>	<p>Het door overheden voldoen aan de BIO is nu een interbestuurlijke afspraak. Er zijn plannen om dit in wetgeving te gaan verankeren. Voor het zorgbedrijf geldt dat het voldoen aan de NEN7510 reeds in wetgevingen opgenomen is. Dit betekent dat er steeds meer van inspanningsverplichting naar resultaatverplichting geschoven wordt en dit derhalve een steeds belangrijker onderdeel in de bedrijfsvoering van VRF gaat worden.</p> <p>Verder zien we de dat ook de dreigingen van o.a. verstoringen, sabotage en diefstal van informatie en informatievoorziening alleen maar toenemen. VRF zal dus steeds meer dan voorheen uitgedaagd worden om informatieveiligheid gedegen in haar organisatie in te bedden en tegelijkertijd zal zij ook moeten beseffen dat 100% veiligheid niet bestaat.</p>

Financiële consequenties	Implementatie van dit beleid zal binnen de bestaande begroting van VRF gerealiseerd worden.
Vervolgaanpak/uitvoering	Momenteel loopt er in aansluiting op het zg. 'Versnellingsplan informatieveiligheid' een project bij VRF dat gericht is op het implementeren van de BIO/NEN normen. Dit project loopt eind 2022 af en daarmee zal de uitvoering van dit beleid in de lijn worden belegd.
Communicatie	Bij vaststelling van het beleid door het bestuur zal dit beleid op het Intranet geplaatst en gecommuniceerd worden. Verder zullen er verschillende activiteiten georganiseerd worden gericht op bewust maken en bewust houden van al onze medewerkers.
Besluit	Kies een item.
Paraaf secretaris	
Kopie naar auteur	