Regio
Gooi en Vechtstreek

Strategisch Informatiebeveiligingsbeleid Regio Gooi en Vechtstreek

Van 2019 tot en met 2022

Ons kenmerk	19.0013516
Versie	0.4
Datum	30 oktober 2019
Contactpersoon	
E-mail	@regiogv.nl

Gemeente Blaricum · Gemeente Eemnes · gemeente goorsemaren · Hilversum Mediastad · Gemeente Huizen · Gemeente Laren · Gemeente Weesp · Wijdemeren

INHOUD

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	11 09 2019		
0.2	24 09 2019		Feedback.
0.3	29 10 2019	CMT	Ingestemd
0.4			Instemming DB

Inleiding

Dit document beschrijft het strategische informatiebeveiligingsbeleid van de Regio Gooi en Vechtstreek ('Regio') voor de jaren 2019 tot en met 2022.
Deze document is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2019-2022' zet de Regio een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de Regio te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG.

Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Regio Informatiebeveiligingsplan (vastgesteld door het CMT) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de RVE-managers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van relevante audits. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de Regio en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Ambitie en visie van de Regio op het gebied van informatieveiligheid

De komende jaren zet de Regio in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de Regio en de basis voor het beschermen van rechten van burgers, werknemers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is niet alleen gericht op het beschermen van informatie, maar is tegelijkertijd een 'enabler'. Het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken.
De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Ook gaat het niet alleen over ICT; verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

Strategisch beleid

Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2019 tot en met 2022'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de RVE-managers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit betekent dat bij het maken van keuzes op voorhand én daarna een afweging maakt en informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

De 10 principes voor informatiebeveiliging (zie bijlage)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de organisatie zichzelf oplegt. De principes zijn als volgt:

1. Bestuur en management bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de Regio organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen van de Regio, dan kan dit directe gevolgen hebben voor inwoners, medewerkers, ondernemers en partners van de Regio. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Dreigingsbeeld Informatie Beveiligings Dienst

Het Dreigingsbeeld van de Informatie Beveiligings Dienst (IBD) geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

Informatie uit incidenten en inbreuken op de beveiliging

De Regio kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017 en de toepassing daarvan bij de Regio. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 (en eventueel ook NEN-ISO/IEC 7510:2017 genomen.

Voor de ondersteuning van de Regio bij het formuleren en realiseren van haar informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[1] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan. De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.
Dit document beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan van de Regio'.

Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de Regio en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af. Voor zover van toepassing kunnen specifieke beveiligingseisen gelden op grond van bijzondere wet- en regelgeving. Deze worden in aanvullende documenten geformuleerd.

Uitgangspunten

Het bestuur en management spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de Regio heeft, de risico's die de Regio hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het management geeft een duidelijke richting aan informatiebeveiliging en laat zien dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele Regio. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de Regio en de relevante landelijke en Europese wet- en regelgeving.

Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.

---

[1] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
- Alle informatie en informatiesystemen zijn van belang voor de Regio, bepaalde informatie is van vitaal en kritiek belang. Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Regio hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, study en act' vormen samen het managementsysteem van informatiebeveiliging.
- De Regio stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, 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.

Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
- Het Dagelijks Bestuur van de Regio stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De Algemeen Directeur (met instemming van het CMT) stelt jaarlijks het informatiebeveiligingsplan vast.
- De Algemeen Directeur (daarbij gesteund door het CMT) is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De Algemeen Directeur (daarbij gesteund door het CMT) is verantwoordelijk voor het vragen om informatie bij de RVE-managers en ziet erop toe dat de RVE-managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de Algemeen Directeur met kopie aan het CMT.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen voor zover aanwezig.
- De RVE-managers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Alle medewerkers van de Regio worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- De RVE-managers zien er op toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.

- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. RVE-managers kunnen quickscans informatiebeveiliging uitvoeren om deze risico-afwegingen te kunnen maken, daarbij gefaciliteerd door de CISO.

Randvoorwaarden
Belangrijke randvoorwaarden zijn:
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
  - de uitkomsten van eventuele audits;
  - het dreigingsbeeld van de IBD;
  - De door de RVE-managers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD).

In dit model is het lijnmanagement verantwoordelijk voor de eigen processen, inclusief de informatiebeveiliging daarvan.
De tweede lijn (CISO, security officers indien aanwezig) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt.
In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Aansturing: Algemeen Directeur en Centraal Management Team (CMT)

De Algemeen Directeur (met instemming van het CMT) zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een RVE-manager. De Algemeen Directeur zorgt dat de RVE-managers zich verantwoorden over de beveiliging van de informatie die onder hen berust.

De Algemeen Directeur (met instemming van het CMT) stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De Algemeen Directeur (met instemming van het CMT) draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de Regio GV. De Algemeen Directeur (met instemming van het CMT) autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de Regio gezien als een integraal onderdeel van risicomanagement.

Uitvoering: RVE- managers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle RVE-managers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. RVE-managers rapporteren aan de Algemeen Directeur (met kopie aan het CMT) over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het CMT overleg.

Taken van de RVE-managers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.

- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Voorbereiding en coördinatie van het overleg ligt bij de CISO.

Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het Dagelijks Bestuur van de Regio. Het Dagelijks Bestuur, de Algemeen Directeur, het CMT en de RVE-managers zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De Algemeen Directeur (daarbij gesteund door het CMT) is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het Dagelijks Bestuur. De Algemeen Directeur (daarbij gesteund door het CMT) rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische onderwerpen die aanvullend zijn op dit strategische beleid.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking waarmee het Dagelijks Bestuur aangeeft in hoeverre de Regio voldoet aan de afspraken die gemaakt zijn en welke eventuele verbetermaatregelen die de Regio gaat treffen.

Middels deze verantwoording wordt het Algemeen Bestuur van de Regio geïnformeerd. Deze essentiële betrokkenheid van het bestuur laat zien dat de Regio informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.