Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Koggenland

2022 tot 2026

Datum: Januari 2022
Auteur: Serena de Boer
Status: V1.7
Classificatie: Openbaar (0)

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.7	24-01-2022	Serena de Boer	Opzet document
0.8	27-01-2022	Ferry Posno	Review
0.9	27-01-2022	Serena de Boer	Verwerken wijzigingen review Ferry Posno.
1.0	03-02-2022	Serena de Boer	Verwerken aantekeningen Eduard Kerssemakers.
1.1	07-02-2022	Serena de Boer	Verwerken aantekeningen Tim Koenders.
1.2	09-02-2022	Serena de Boer	Verwerken aantekeningen Maarten van Rooij.
1.3	14-02-2022	Serena de Boer	Verwerken feedback n.a.v. overleg met Eduard Kerssemakers en Tim Koenders op 10-02-2022.
1.4	23-02-2022	Serena de Boer	N.a.v. MT-voorstel, verwerken feedback van Marc Winder.
1.5	04-04-2022	Serena de Boer	N.a.v. DMT voortel, verwerken feedback DMT op 29-03-2022.
1.6	20-04-2022	Serena de Boer	N.a.v. overleg met Tim Koenders, verwerken feedback.
1.7	17-05-2022	Serena de Boer	Strategisch Gemeentelijk Informatiebeveiligingsbeleid is op 17 mei 2022 vastgesteld door het College van Gemeente Koggenland.

Inhoudsopgave

Managementsamenvatting

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2022 tot en met 2025. Met dit 'strategisch Informatiebeveiligingsbeleid 2022-2026' zet de gemeente Koggenland een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en door te gaan met de stappen die in de voorgaande jaren zijn gezet. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO).

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen met als doel om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere gevoelige informatie te waarborgen binnen de organisatie. Het is de primaire verantwoordelijkheid van de afdelingshoofden om de eigen processen, systemen en gegevens te beveiligen en hier voldoende middelen voor beschikbaar te stellen. En de benodigde maatregelen uit het jaarplan (privacy - informatiebeveiliging) uit te voeren. De CISO en de ISO adviseren, coördineren en ondersteunen hierbij. Advies omtrent privacy en gegevensbescherming wordt gegeven door de collegae Privacy Officer en Functionaris Gegevensbescherming van gemeente Koggenland.

De colleges van de gemeenten Koggenland, Opmeer en Medemblik hebben sinds 2015 de ambtelijke samenwerking geïntensiveerd. De voornaamste redenen daarvoor was het delen van (specialistische) kennis, eventueel lagere kosten en het verminderen van de kwetsbaarheid van de organisaties.

De huidige vijf thema's waarop wordt samengewerkt zijn (vakgebied bedrijfsvoering) o.a.:

- Inkoop & contractmanagement;
- Personeel en Organisatie;
- Gemeenschappelijke bezwarencommissie;
- Informatiemanagement en beheer;
- Informatiebeveiliging en privacy.

Naast deze samenwerking zijn gemeenten Koggenland en Opmeer een samenwerking aangegaan op het gebied van informatievoorziening; de I-samenwerking. Doel om continuïteit te waarborgen, efficiëntie te verhogen en kwetsbaarheid verminderen. Het informatiebeveiligingsbeleid is separaat opgesteld, maar ligt zowel voor gemeente Koggenland als voor gemeente Opmeer op een lijn.

SSC DeSom faciliteert, ondersteund en onderhoud voor gemeente Koggenland de ICT-omgeving. Deze regionale samenwerking aan duurzame ICT-oplossingen draagt bij aan een betere dienstverlening aan burgers en bedrijven. Door kennis en kracht te bundelen, bouwen en ontwikkelen de partijen samen, digitale oplossingen die de dienstverlening aan burgers en bedrijven ondersteunen en verbeteren.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de Informatievoorziening gedurende de gehele levenscyclus van informatiesystemen. Het beperkt zich echter niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, inwoners, gasten/bezoekers en externe relaties.

Informatie is een belangrijk bedrijfsmiddel. Beveiliging van deze informatie is nodig om een goede en veilige dienstverlening naar burgers, bedrijven en ketenpartners te garanderen. Daarom is het volgende algemene doel gesteld voor de informatiebeveiliging:

De gemeente Koggenland is een betrouwbare partner voor al haar burgers, bedrijven en ketenpartners.

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 (fysieke) toegang;
- Het beheersen van de toegang tot informatiesystemen;
- Het garanderen van betrouwbare en veilige informatievoorzieningen;
- Het waarborgen van veilige informatiesystemen;
- Het adequaat reageren op incidenten;
- Het beschermen van kritieke bedrijfsprocessen;
- Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers;
- Het waarborgen van de naleving van dit beleid.

De gemeente zet de komende jaren in op het optimaliseren van de informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie(s).

Een solide inrichting van informatiebeveiliging aan de voorkant voorkomt gedoe achteraf. Om deze solide inrichting te bereiken, is het noodzakelijk om op het gebied van informatieveiligheid te professionaliseren. Het huidige volwassenheidsniveau van informatiebeveiliging van gemeente Koggenland ligt op niveau 1. De ambitie is om eind 2025 volwassenheidsniveau 4 (figuur 1) te bereiken. Zodra dat niveau bereikt is, heeft de organisatie informatieveiligheid geborgd binnen haar processen. Zij voldoet aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda. Het volwassenheidsniveau wordt jaarlijks geëvalueerd.

Figuur 1: volwassenheidsniveau

De volwassenheidsniveau's zijn gekoppeld aan het document: ''Stip op de Horizon''. Dit document vormt in lijn met de BIO een jaaroverzicht en planning.

1 Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2022 tot 2026 en vervangt het in 2019 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2019 tot 2023'.

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Dit document treedt in werking na formele goedkeuring van het managementteam en college van B&W.

Dit strategisch informatiebeveiligingsbeleid sluit aan bij de visie van de gemeente om goed in verbinding te staan met inwoners, ondernemers en samenwerkingspartners om optimale (digitale) dienstverlening te bieden. We werken met veilige digitale systemen en benutten de techniek verantwoord. Met behulp van data kunnen we leren en verbeteren. Zo streven we naar een steeds betere (digitale) dienstverlening.

Doelstelling:
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid.

Resultaat:
Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

Met dit ''Strategisch Gemeentelijk Informatiebeveiligingsbeleid van 2022 tot 2026" zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente 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) [1]. Op basis van De 10 bestuurlijke principes voor informatiebeveiliging [4], de Handreiking Informatiebeveiligingsbeleid BIO [2] en het Voorbeeld Strategisch Gemeentelijk Informatiebeveiligingsbeleid BIO [3] is dit strategisch informatiebeveiligingsbeleid opgesteld. Dit beleid wordt minimaal één keer per drie jaar beoordeeld op actualiteit (BIO 5.1.2.1).

In 2022 wordt richting gegeven aan zienswijze, implementatie BIO (uitwerken documentatie) en awareness voor gemeente Koggenland. 2022 tot en met 2025 staan in het teken van de ambitie om eind 2025 volwassenheidsniveau 4 te bereiken. Zodra dat niveau bereikt is, heeft de organisatie informatieveiligheid geborgd binnen haar processen. Zij voldoet aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen. Zij weet haar risico's te verkleinen tot een acceptabel niveau in lijn met de ambities uit de strategische agenda.

1.1 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 gemeentelijk Informatiebeveiligingsplan (afdelingsplannen) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingshoofden/ teamleiders, de CISO en ISO (PO en FG), het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. 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.

1.2 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 gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

Kernpunten van informatiebeveiliging zijn:

- Beschikbaarheid (of continuïteit): het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit: het waarborgen van de correctheid (juistheid), volledigheid, tijdigheid van informatie en informatieverwerking oftewel het in overeenstemming zijn van informatie met de werkelijkheid;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe bevoegd en geautoriseerd zijn;
- Controleerbaarheid: waarborgen dat de beoogde toegang tot gegevens en de juiste werking van systemen continu alsook achteraf te controleren is.

1.3 Ambitie en visie van de gemeente op het gebied van informatieveiligheid

De hoofddoelstelling van dit informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente. Er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en middelen aangegeven waarmee dit beleid moet worden vormgegeven.

Informatie is een belangrijk bedrijfsmiddel dat de gemeente Koggenland op gepaste wijze wil beschermen. Daarom is het volgende doel gesteld voor informatiebeveiliging:

De gemeente Koggenland is een betrouwbare partner voor al haar burgers, bedrijven en ketenpartners.

De gemeente zet daarom de komende jaren in op het optimaliseren van de informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie.

2 Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het ''Strategisch Informatiebeveiligingsbeleid voor de jaren 2022 tot 2026''. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (afdelingsplannen).

2.2 Ontwikkelingen

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

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. Deze baseline is een vertaling van de internationale informatieveiligheidsnormen NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017. Of anders gezegd, de BIO is gebouwd rondom de ISO27001 met verwijzingen naar maatregelen uit de ISO27002. Implementatie van de BIO impliceert dat ook voldaan moet worden aan (delen van) de informatieveiligheidsstandaard ISO270002.

De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de afdelingshoofden/ teamleiders nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Risicomanagement is een middel om op een gestructureerde manier risico's in kaart te brengen, te evalueren en – door er proactief mee om te gaan – beter te beheersen. De organisatie inventariseert risico's en de gevolgen van de risico's en verbindt er maatregelen aan.

2.2.2 De 10 principes voor informatiebeveiliging (zie [4])

Informatieveiligheid is een organisatie breed aandachtspunt. Het is in feite een kwaliteitsaspect dat in alle processen van de organisatie terugkomt. Dit is de reden dat we informatieveiligheid niet als een geïsoleerd onderwerp kunnen benaderen.

Naast de 10 principes van informatiebeveiliging hanteert de gemeente Koggenland ook strategische doelen, deze worden behandeld in paragraaf 2.6.1.

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader [1] BIO en gaan over de waarden die de portefeuillehouder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders 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;

[1] Deze principes worden gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG).

10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke 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 gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten [5] (figuur 2) 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.

De gemeentelijke informatievoorziening van gemeente Koggenland en daarbij de faciliterende ICT partij SSC DeSom is kwetsbaar. We onderscheiden daarin een aantal categorieën van dreigingen in volgorde van belangrijkheid:

- Intern en onbedoeld;
- Extern, bedoeld maar ongericht;
- Extern, bedoeld en gericht;
- Intern en bedoeld.

Figuur 2: dreigingsbeleid.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente 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.

2.3 Standaarden informatiebeveiliging

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

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] 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-normering en de BIO. Ook het Informatiebeveiligingsplan (afdelingsplannen) zal deze structuur volgen.

Binnen de gemeente wordt naast ICT, ook Operationele Technologie (OT) ingezet, hiermee worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering (PA). Binnen het beveiligingsbeleid van de gemeente is ook ruimte voor de bescherming van PA, en dit beleid betreft dan ook beleidsafdelingen (SSC DeSom) die zich met PA bezighouden.

2.4 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.

Deze nota 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 'Gemeentelijk Informatiebeveiligingsplan' (afdelingsplannen).

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt ook aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

Bewust wordt in het strategisch beleid geen overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

Het beleid is opgesteld met inachtneming van de toekomstvisie, missie en kernwaarden van de gemeente Koggenland en het nieuwe coalitieprogramma.

Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen:

- Autorisatiebeleid;
- ICT ontwerp(en);
- Beleid leveranciers/externe partijen;

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

- Bedrijfsprocessen;
- Beheerrichtlijnen ICT;
- Patchbeheer-beleid;
- Configuratiebeheer;
- Continuïteitsbeheer;
- Interne controle;
- Fysieke beveiliging (beveiliging die met behulp van fysieke middelen gerealiseerd wordt);
- Gedragsregels;
- HR-proces;
- Incidentenbeheer;
- Loggingbeleid;
- Wijzigingsproces.

De uitwerking van het beleid in concrete te nemen maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (afdelingsplannen).

2.5.1 Relatie met privacy

Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacy zijn echter twee verschillende begrippen. Ze hebben wel een gemeenschappelijk raakvlak. Informatiebeveiliging heeft een bredere scope dan de bescherming van enkel persoonsgegevens.

Informatiebeveiliging draait om de bescherming van alle gevoelige informatie tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn.

Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywet. Artikel 32 van de AVG schrijft voor dat:

"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen".

Informatiebeveiliging maakt daarmee een onderdeel uit van de AVG. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Wel geeft de AVG-voorbeelden van mogelijke risico's en maatregelen. Normenkaders als de BIO helpen de gemeente om de risico's goed in te schatten en de benodigde maatregelen te treffen. Hoe de gemeente omgaat met privacy en de AVG is beschreven in de privacyverklaring van de gemeente Koggenland.

2.6 Uitgangspunten

Het bestuur, het managementteam en het afdelingsmanagement 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 gemeente hebben, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan is dit beleid voor informatiebeveiliging opgesteld door de ISO. Het beleid wordt uitgedragen naar de organisatie, wordt ondersteunt en de uitvoering ervan wordt bewaakt.

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

2.6.1 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;
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

Gemeenten Koggenland en Opmeer zijn een samenwerking aangegaan op het gebied van informatievoorziening; de I-samenwerking. Doel om continuïteit te waarborgen, efficiëntie te verhogen en kwetsbaarheid verminderen. Het informatiebeveiligingsbeleid is separaat opgesteld, maar ligt zowel voor gemeente Koggenland als voor gemeente Opmeer op een lijn.

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. De portefeuillehouder is eindverantwoordelijke voor de informatiebeveiliging.
- Het beleid is tevens van toepassing op alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Koggenland 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 (afdelingsplannen) het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan (afdelingsplannen) 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, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om hun 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.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B&W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- Het managementteam stelt jaarlijks het informatiebeveiligingsplan (afdelingsplannen) vast.
- Het managementteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.

- Het managementteam is verantwoordelijk voor het vragen om informatie bij de teamleiders en ziet erop toe dat de teamleider adequate maatregelen genomen hebben voor de bescherming van de informatie, informatiesystemen en procesautomatiseringsystemen 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 het afdelingshoofd bedrijfsvoering, voorafgaand aan de P&C-gesprekken. Waarna de ISO deze informatie zal ontvangen.
- 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 ook worden opgenomen in de auditplannen.
- De teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teamleiders zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- De ISO-medewerker draagt zorg voor de implementaties van de beleidsstukken in de compliance tool. Samen met de PO en FG van de gemeente vormt de ISO een team.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Teamleiders dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teamleiders voeren QuickScans informatiebeveiliging uit op basis van de BIO (BBN-toetsen) om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.6.4 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 (afdelingsplannen) opgesteld onder leiding van de CISO, gebaseerd op:
    - Information Security Management System (ISMS) – GRC-tool CyberManager;
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Het dreigingsbeeld gemeenten van de IBD;
    - De door de afdelingshoofden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse.

3 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. De tweede lijn (CISO, ISO-medewerker en PO en FG) ondersteunt, adviseert, coördineert en bewaakt of de teamleiders en het managementteam 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.

3.1 Aansturing: managementteam

Het managementteam zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder een afdelingshoofd vallen, welke zijn of haar verantwoordelijkheid delegeert aan een teamleider en of teamleiders. De afdelingshoofden zorgen dat de teamleider en of teamleiders zich verantwoorden over de beveiliging van de informatie die onder hen berust. Het managementteam zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad. Het Afdelingshoofd Bedrijfsvoering, is eerste aanspreekpunt- verantwoordelijk als het gaat om aansturing.

Het managementteam stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het managementteam draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan en ondersteunen door de CISO en ISO (PO en FG) van de gemeente. Het managementteam autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Koggenland gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: teamleiders

Informatiebeveiliging valt onder de verantwoordelijkheden van alle teamleiders. 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. Teamleiders rapporteren via de afdelingshoofden aan het bestuur 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 breed (groot) managementteam overleg.

Taken van de teamleiders (die ondersteund wordt door de ISO van de gemeente Koggenland) in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures;
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is;
- 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.

3.3 Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente Koggenland. De bestuurders, het management en afdelingshoofden/ teamleiders van de gemeente Koggenland 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. Met het uitgangspunt dat de teamleiders verantwoordelijk zijn en het management vooral dient al het escalatieniveau.

Het managementteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het managementteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. Deze rapportages zijn afkomstig van de teamleiders, welke zijn gegenereerd door de CISO en ISO.

3.3.1 Borging van het informatiebeveiligingsbeleid

Om de borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen, onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA-cyclus resulterend in een Information Security Management System (ISMS) [18.2.1.1] (zie figuur 1):

1. Informatieveiligheidsbeleid (zowel strategisch als tactisch):

Stap 1 bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Dit is een organisatie breed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar voor het bestuur en managementteam, dit wordt ook wel het 'pas toe of leg uit' principe genoemd. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 3 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats [5.1.2.1];

2. Informatieveiligheidsanalyse:

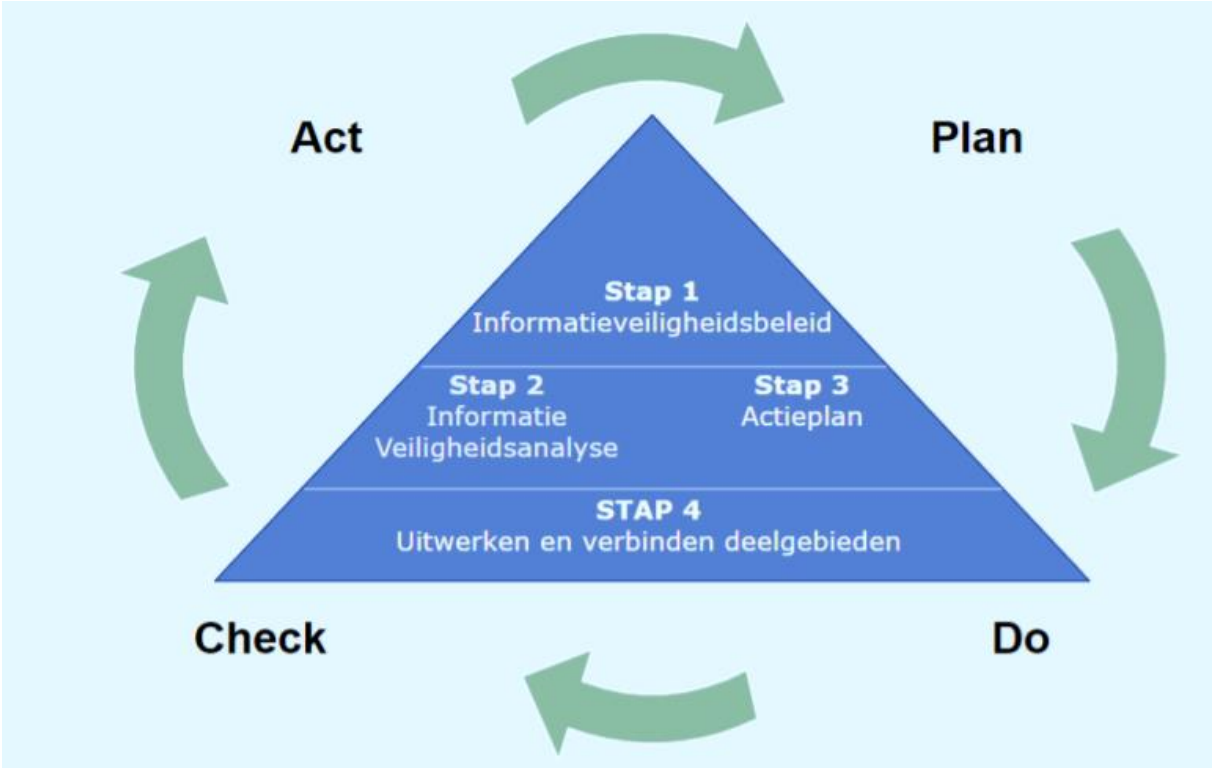
Stap twee is gericht op het implementatietraject van de gemeente Koggenland. De implementatiefase begint met het uitvoeren van een informatieveiligheidsanalyse. Hiertoe wordt allereerst een overzicht opgesteld van de gegevensverzamelingen/applicaties in de gemeentelijke organisaties door de CISO. Deze worden toegewezen aan een eigenaar en geclassificeerd op de risicoklassen beschikbaarheid, integriteit en betrouwbaarheid van de informatie (ook wel dataclassificatie genoemd). Ook wordt het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld. Hierbij geldt dat gemeente breed het BBN2 wordt gehanteerd. Hiervan kan slechts bij individuele informatiesystemen en mits voldoende beargumenteerd (vastgelegd), worden afgeweken. Hierna wordt de praktijksituatie in de gemeente getoetst aan het gemeente brede informatieveiligheidsbeleid en aan de beveiligingsmaatregelen uit de BIO, met het uitvoeren van een GAP-analyse, rondgang door het gebouw, evaluatie ENSIA en een (eventuele) evaluatie van het vorige actieplan. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar.

3. Actieplan Informatieveiligheid (informatiebeveiligingsplan of wel afdelingsplannen):

Op basis van de informatieveiligheidsanalyse wordt in stap drie een actieplan opgesteld. De in de analyse geconstateerde risico's worden gewogen en waar nodig van maatregelen voorzien. Prioritering van de acties wordt gedaan op basis van de risico's die zijn geconstateerd, de beschikbare tijd en de beschikbare middelen. Hierdoor ontstaat een compact actieplan waarmee de gemeente vaststelt welke verbeteracties gedurende een periode van 1 of 2 jaar worden uitgevoerd. Dit actieplan vormt een praktische leidraad voor de verbetering en borging van informatieveiligheid in de organisatie. De gemeente komt bij elkaar om de implementatie van het actieplan informatieveiligheid (afdelingsplannen) te evalueren te bewaken en waar nodig bij te stellen. Dit vindt conform de bespreking in het breed (groot) managementteam overleg (zie paragraaf 3.2) minimaal tweemaal per jaar plaats.

4. Technische en organisatorische maatregelen:

Stap vier bestaat uit het opleveren van een complete set aan technische en organisatorische maatregelen die gericht is op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO, maar ook om applicaties zoals de BRP, SUWI, de BAG, het financiële systeem, of om de primaire processen van de organisatie, ICT-beheerprocessen of de inrichting van de ICT-platformen. Dit betreft met name het opstellen van procedures en werkinstructies.



Figuur 1: PDCA-cyclus

3.3.2 ENSIA

De gemeente verantwoord zich over informatiebeveiliging middels de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). De ENSIA-coördinator voor gemeente Koggenland is de CISO, de ISO van de gemeente biedt ondersteuning. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke afdelingshoofden. De afdelingshoofden leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording wordt het college van de gemeente Koggenland en de gemeenteraad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Koggenland informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

4 Bevordering beveiligingsbewustzijn

Informatiebeveiligingsbeleid is niet iets dat wordt gemaakt om in de kast te leggen. Een goed informatiebeveiligingsbeleid wordt beoogd de basis te leggen voor goede informatieveiligheid binnen de gemeente. Niet alle delen van het informatiebeveiligingsbeleid van de gemeente zijn voor alle doelgroepen binnen de gemeente even belangrijk. En ook niet alle doelgroepen zullen hetzelfde kennisniveau (hoeven) hebben. De gemeente onderscheid daarom verschillende doelgroepen. De volgende doelgroepen worden onderscheiden:

1. De medewerkers die werken met de informatie(systemen)
2. Beheerders van informatie(systemen)
3. Bestuurders, managementteam en afdelingsmanagement

1. De medewerkers die werken met de informatiesystemen

Door het houden van bewustwordingscampagnes wordt structureel invulling gegeven aan het informeren van de medewerkers binnen de gemeente over de algemene beginselen van informatiebeveiliging die iedere medewerker zou moeten kennen en toepassen. Hier wordt invulling aan gegeven door het plaatsen van berichten op het intranet, het geven van workshops of het beschikbaar stellen van e-learning.

2. Beheerders van informatiesystemen

Dit betreft de technisch- en functioneel applicatiebeheerders.
Specifieke aandachtspunten voor de beheerders zijn:

- De bijzondere positie van de beheerder en de gevaren;
- Omgang met beheerdersaccounts, autorisaties en wachtwoorden;
- Dataclassificatie (passende bescherming van gevoelige gegevens zoals persoonsgegevens);
- Back-up en restore;
- Beheren op afstand;
- Bedrijfscontinuïteit;
- Open standaarden (Forum Standaardisatie);
- IT-beveiligingsprocessen en procedures zoals incidentmanagement, CMDB, wijzigingsbeheer etc.

3. Bestuurders, managementteam en afdelingsmanagement

Onderwerpen die van belang zijn voor hoofden, leidinggevenden en bestuurders:

- Beveiligingsverantwoordelijkheden van het afdelingshoofd;
- Personeelsprocessen (in dienst, uit dienst en functiewisselprocessen);
- Beveiliging en projecten;
- Risicomanagement;
- Bedrijfscontinuïteit en crisisbeheersing;
- Beveiliging en inkoop;
- Dataclassificatie;
- Privacy;
- Verantwoording over beveiliging (ENSIA).

Naast het kunnen beschikken over de juiste middelen, vraagt bovenstaande om een bewuste houding. Bewust van de kansen die digitaal werken biedt voor de medewerkers en voor burgers en bedrijven. En bewust van de risico's ten aanzien van de vertrouwelijke gegevens en de middelen waarmee die kansen worden gerealiseerd.

Die bewuste houding ontstaat niet vanuit het niets. Medewerkers worden geïnformeerd over de aanwezigheid van ondersteunende middelen en hoe deze praktisch en veilig benut kunnen worden. En medewerkers worden geïnformeerd over de mogelijke bedreigingen waaraan onze informatiehuishouding tegenwoordig bloot staat. Waarbij uiteraard ook wordt geleerd hoe deze bedreigingen het hoofd te bieden. Deze start is in 2022 reeds gemaakt doormiddel van het awareness – traingingsprogramma Infosequre, welke medio juni wordt vervangen door Arda. Waar alle medewerkers middels trainingen op het gebied van cybercrime kunnen volgen. O.a. de onderwerpen phishing, social enginering en veilig werken vanuit huis komen hier aan bod.

De informatiebeveiliging kan immers nog zo goed op orde zijn, deze valt of staat op basis van de kennis en bewustwording en de houding en het gedrag van de medewerkers die met de informatie werken. Het is de verantwoordelijkheid van iedere medewerker om de aangeboden kennis tot zich

te nemen en toe te passen. En het is aan de leidinggevenden om deze professionele houding te ondersteunen en waar nodig te stimuleren.

Referenties

#	Referentie	Document/ URL
1	Baseline Informatiebeveiliging Overheid (BIO)	https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
2	Handreiking Informatiebeveiligingsbeleid BIO	https://www.informatiebeveiligingsdienst.nl/product/handreiking-informatiebeveiligingsbeleid-bio/
3	Voorbeeld Strategisch Gemeentelijk Informatiebeveiligingsbeleid BIO	https://www.informatiebeveiligingsdienst.nl/product/voorbeeld-strategisch-gemeentelijk-informatiebeveiligingsbeleid/
4	De 10 bestuurlijke principes voor informatiebeveiliging	https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/
5	Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten	https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2021-2022/