Strategisch Informatiebeveiligingsbeleid

Gemeente Kapelle

Gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO)

BIO-maatregel: 5.1.1.1
Documentversie: 1.0
Datum: 03-06-2020

Vastgesteld door het college van B&W van de gemeente Kapelle op: 7 juli 2020

Inhoud

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid vanaf 2020 en vervangt het in 2017 vastgestelde 'Gemeentebreed Informatiebeveiligingsbeleid 2017-2019'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit strategisch informatiebeveiligingsbeleid 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), zie bijlage A. De principes zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage B.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het informatiebeveiligingsplan, waarvoor de BIO-GAP-analyse het raamwerk vormt, worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingshoofden, de CISO's van de Bevelandse gemeenten en GR de Bevelanden, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. In het informatiebeveiligingsplan worden dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Dit gebeurt in nauwe afstemming tussen de Bevelandse gemeenten en GR de Bevelanden en is zoveel mogelijk uniform. De gemeente Kapelle volgt daarmee het gezamenlijk afgestemde beleid in de Bevelanden. Alleen daar waar verantwoordelijkheden gemeentespecifiek zijn, worden deze apart voor de gemeente Kapelle uitgewerkt en in het MT besproken en afgestemd.
Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.
Aan het einde van dit document is een lijst met veelgebruikte afkortingen toegevoegd.

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.

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

De gemeente Kapelle zet in op het verder verhogen van informatieveiligheid. Voor de inrichting van informatiebeveiliging wordt de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van personen en organisaties. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

De gemeente zorgt ervoor te kunnen voldoen aan wettelijke verplichtingen op het gebied van informatieveiligheid. Binnen de afdelingen moet duidelijk zijn welke eisen er gelden op het gebied van beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van de gegevens en processen.

De komende jaren wordt ingezet op het opstellen, of waar nodig bijstellen, van tactisch beleid voor onderwerpspecifieke aandachtsgebieden, in overeenstemming met de BIO. Om informatiebeveiligingseisen af te dekken, worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd. De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging.

2. Strategisch beleid

2.1. Doel

Het doel van deze beleidsnota is het presenteren van het strategisch informatiebeveiligings-beleid vanaf 2020. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het doorlopend bij te stellen informatiebeveiligingsplan, waarvoor de BIO-GAP-analyse het raamwerk vormt.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligings-beleid zijn de volgende:

2.2.1 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 (Baseline Informatiebeveiliging Gemeenten). Dat wil zeggen dat de afdelingshoofden nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt 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.

2.2.2 De 10 bestuurlijke principes voor informatiebeveiliging

De 10 bestuurlijke principes voor informatiebeveiliging[1] (zie bijlage B) zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder 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.
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.

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

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

De IBD heeft inzicht in incidenten en trends en publiceert tweejaarlijks een Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten (zie bijlage C). Dit Dreigingsbeeld geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld geeft daarmee input om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

Naast het hierboven genoemde dreigingsbeeld kent de gemeente, gezamenlijk met de andere Bevelandse gemeenten en GR de Bevelanden, een eigen systeem waarin incidenten worden vastgelegd. Incidenten uit het verleden kunnen waardevolle informatie geven om van te leren en kunnen benut worden als 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 brengt de IBD praktische operationele handreikingen uit.
De inhoud en structuur van deze nota zijn afgestemd op die van de ISO 27001/27002 en de BIO. Ook het informatiebeveiligingsplan zal deze structuur volgen.

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 op te stellen en doorlopend bij te stellen informatiebeveiligingsplan. Deze tactische en operationele aspecten van informatieveiligheid worden in nauw overleg met de Bevelandse gemeenten en GR de Bevelanden opgesteld en zoveel mogelijk geüniformeerd.

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

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, 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 informatiebeveiligingsbeleid is een algemene basis en vormt als overkoepelend beleid de kapstok voor aanvullend beleid, procedures en richtlijnen. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog domeinspecifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze zijn in aanvullende normen en richtlijnen geformuleerd, waarvoor de verantwoordelijkheid ligt bij de proceseigenaar voor het betreffende domein.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen, omdat wet- en regelgeving aan verandering onderhevig is. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het bestuur, de directeur/gemeentesecretaris en de afdelingshoofden spelen een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid. Afdelingshoofden maken 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 zijn. Op basis hiervan dragen afdelingshoofden het informatiebeveiligings-beleid uit naar de organisatie en ondersteunen de uitvoering ervan.

Met het uitdragen en handhaven van dit beleid geeft de gemeente een duidelijke richting aan informatiebeveiliging. Alle medewerkers demonstreren dat zij informatiebeveiliging ondersteunen en zich hierbij betrokken voelen. 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 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

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. Het college van B&W is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van alle medewerkers. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Kapelle 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 proceseigenaar.
- De verantwoordelijkheid voor de beveiliging van de technische omgeving die door GR de Bevelanden wordt beheerd, ligt bij het hoofd van de afdeling ICT van GR de Bevelanden.
- Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligings-plan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt doorlopend 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. Daarnaast zijn inspireren, mobiliseren, waarderen en reflecteren (IMWR) van belang voor de menselijke factor in de verbetercyclus. Dit komt tot uitdrukking in iBewustzijn: medewerkers die bewust en zorgvuldig omgaan met (persoons)gegevens en gevoelige of vertrouwelijke informatie.
- De gemeente 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.

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.
- De directeur/gemeentesecretaris is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerpspecifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. Dit gebeurt op basis van het informatiebeveiligingsplan, waarvoor de BIO-GAP-analyse het raamwerk vormt.
- De directeur/gemeentesecretaris is verantwoordelijk voor het vragen om informatie bij de vakafdelingen en ziet erop toe dat de proceseigenaars adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) adviseert, coördineert en houdt toezicht vanuit een onafhankelijke positie en ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directeur/gemeentesecretaris, voorafgaand aan de P&C-gesprekken.
- 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, zijn opgenomen in de auditplannen binnen ENSIA.

- De proceseigenaars zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging binnen hun domein.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT, BRO) 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.
- Alle medewerkers van de gemeente zijn getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- De CISO ziet erop toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd. Afdelingshoofden dienen te kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben, o.a. door periodieke controle van autorisaties.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden verlenen medewerking aan de uitvoering van quickscans informatiebeveiliging op basis van de BIO om deze risico-afwegingen te kunnen maken.

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.
- Het informatiebeveiligingsplan, waarvoor de BIO-GAP-analyse het raamwerk vormt, wordt doorlopend bijgesteld door de CISO, in afstemming met de collega-CISO's in de Bevelandse gemeenten en GR de Bevelanden, gebaseerd op:
    - 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;
    - in het Deelnemersoverleg Informatiebeveiliging (DIB, Bevelandse gemeenten en GR) ingebrachte onderwerpen. Het DIB is een periodiek overleg van de CISO's van de Bevelandse gemeenten en GR de Bevelanden.

2.7 Evaluatie strategisch informatiebeveiligingsbeleid

Het strategisch informatiebeveiligingsbeleid wordt bij belangrijke wijzigingen als gevolg van reorganisatie of wet- en regelgeving geëvalueerd en zo nodig bijgesteld. Minimaal eens per 3 jaar wordt beoordeeld of dit noodzakelijk is.

3. Organisatie, taken en 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) ondersteunt, adviseert, coördineert en bewaakt of iedereen zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directeur/gemeentesecretaris

De directeur/gemeentesecretaris zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De directeur/gemeentesecretaris zorgt dat de proceseigenaars/vakafdelingen zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directeur/gemeentesecretaris zorgt dat de eindverantwoordelijke portefeuillehouder binnen het college gevraagd en ongevraagd geïnformeerd wordt 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.

De directeur/gemeentesecretaris stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast of delegeert dit aan de afdelingshoofden. De directeur/gemeentesecretaris draagt zorg voor het laten uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen door de CISO van de gemeente. De directeur/gemeentesecretaris autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Kapelle gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: alle medewerkers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle medewerkers. Medewerkers vertonen voorbeeldgedrag en kunnen elkaar aanspreken op mogelijk (onbewust) onveilig gedrag. Daarmee leveren alle medewerkers een belangrijke bijdrage aan iBewustzijn van de hele organisatie. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Vakafdelingen rapporteren over de door hen uitgevoerde informatiebeveiligings-activiteiten binnen hun domein. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken met de CISO/ENSIA-coördinator in het kader van ENSIA. Voorbereiding en coördinatie van het overleg ligt bij de CISO/ENSIA-coördinator.

Taken van de proceseigenaars/vakafdelingen 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 en 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 informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de gemeente Kapelle. De bestuurders en directeur/gemeentesecretaris van de gemeente Kapelle zullen volgens de 10 bestuurlijke principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging.
De CISO kan gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de portefeuillehouder en de gemeentesecretaris. De CISO rapporteert daarnaast over de mate waarin de organisatie invulling geeft aan het uitwerken van tactische (deel)beleidsonderwerpen die aanvullend zijn op dit strategisch beleid.

3.3.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Daarvoor is een ENSIA-coördinator aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaars/vakafdelingen. De vakafdelingen leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt tot uitdrukking in het jaarverslag en in de collegeverklaring ENSIA. Met deze verklaring geeft het college van B&W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording over 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 worden het bestuur van de gemeente Kapelle en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Kapelle informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Veelgebruikte afkortingen

BAG	Basisregistratie Adressen en Gebouwen
BGT	Basisregistratie Grootschalige Topografie
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BRO	Basisregistratie Ondergrond
BRP	Basisregistratie Personen
CISO	Chief Information Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
GR	Gemeenschappelijke Regeling Samenwerking de Bevelanden
IBD	Informatiebeveiligingsdienst Gemeenten
ICT	(afdeling) Informatie- en communicatietechnologie
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NCSC	Nationaal Cyber Security Centrum
NEN	NEderlandse Norm, Nederlands Normalisatie Instituut
P&O	Afdeling Personeel en Organisatie
PDCA	Plan, Do, Check, Act
PNIK	Paspoorten en Nederlandse Identiteitskaarten
PUN	Paspoortuitvoeringsregeling Nederland
SUWI	Wet Structuur Uitvoeringsorganisatie Werk en Inkomen

Bijlage A: Baseline Informatiebeveiliging Overheid (versie 1.04)

https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Bijlage B: De 10 bestuurlijke principes voor informatiebeveiliging

https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

Bijlage C: Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020

https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2019-2020/