

Strategisch Gemeentelijk Informatiebeveiligingsbeleid

Gemeente Stede Broec

2020 – 2025

Auteurs: Berend de Vries (extern)
Paul Gijben (FG)

Datum: 22 oktober 2020

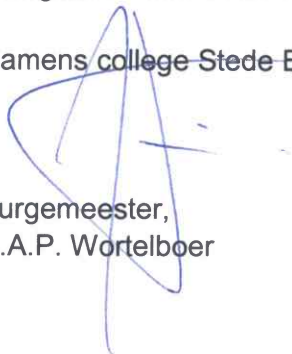
Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	Juli 2020	B.J. de Vries	Eerste opzet
0.2	Augustus 2020	Margreet Smit Paul Gijben	Aanpassingen inhoudelijk
0.3	Augustus 2020	B.J. de Vries	Aanpassingen
0.9	Oktober 2020	Jeroen Broeders	Opmerkingen en aanvullingen betreffende sturing colleges
1.0	Oktober 2020	B.J. de Vries Paul Gijben	Definitief

Vastgesteld d.d. 11 november 2020

Namens college Stede Broec,

Burgemeester,
R.A.P. Wortelboer



Gemeentesecretaris,
A. Huisman



1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot 2025 en vervangt alle eerder vastgestelde Gemeentelijk Informatiebeveiligingsbeleid documenten.

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2025' 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).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld door het Informatiebeveiligingsbeleid SED. In het jaarlijks uit te brengen Informatiebeveiligingsplan SED worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt, onder andere, gedaan op basis van input van de afdelingsleidinggevenden, de CISO, 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 en -processen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT, ook de "papier" informatiestromen en gedrag vallen er onder. Informatiebeveiliging 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 houdt zich aan de wettelijke voorschriften in het omgaan met informatie. De bescherming van de gegevens van inwoners heeft zeer hoge prioriteit. De ambitie van de gemeente is dan ook om niet alleen op papier aan de BIO te voldoen maar om in de praktijk de best mogelijke bescherming van deze gegevens te realiseren. De gemeente heeft het beheer van de gegevens, en daarmee de bescherming van de gegevens, als taak gemandateerd aan de SED.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2020 tot 2025'. Het Gemeentelijk Informatiebeveiligingsbeleid (IBBeleid Gemeente) is kaderstellend voor het Informatiebeveiligingsbeleid van het gemeenschappelijk uitvoeringsorgaan, de SED (IBBeleid SED). De uitwerking van het beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen Informatiebeveiligingsplan (IB-Plan SED).

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 normenkader voor informatiebeveiliging voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de voormalige BIG.

In de BIO wordt de verantwoordelijkheid voor de informatiebeveiliging, net als in de BIG, belegd bij het College van Burgemeester en Wethouders.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader ¹ 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 heeft 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 Verenigde Nederlandse Gemeenten (VNG)

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 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.

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 waardevolle informatie om van te leren en dus zijn incidenten uit het verleden nadrukkelijk input bij het actualiseren van het beleid. Het systeem wordt, in ieder geval voor wat betreft de informatiebeveiliging, gevuld en onderhouden door de SED die hieruit regelmatig rapporteert.

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 Normatiek² in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen.

De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

2.4 Plaats van het strategisch beleid

Het strategisch beleid van de gemeente wordt gebruikt om de basis te leggen voor het informatiebeveiligingsbeleid van de SED en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op zowel tactisch als operationeel niveau.

Het afstemmen van de informatiebeveiligingsnota's van de gemeenten en de SED gaat vooraf aan de besluitvorming.

Dit beleid zal worden vertaald in operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan SED'.

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 gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en

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

gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.

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

2.6 Uitgangspunten

Het College van B&W speelt een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Op aangeven van de SED maakt het College een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

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

Het College 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 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 en W is eindverantwoordelijke voor het informatiebeveiligingsbeleid.
- Het vaststellen van het Informatiebeveiligingsbeleid van de gemeente is een verantwoordelijkheid en taak van het College. De Gemeenteraad wordt van het beleid op de hoogte gesteld en krijgt inzage in de verantwoording van de uitvoering van het beleid.
- Het college draagt de verantwoordelijkheid voor de uitvoering van de informatievoorziening en heeft deze gedelegeerd aan de gemeenschappelijke uitvoeringsorganisatie SED.

- Alle informatiebronnen en -systemen die gebruikt worden door de Gemeente 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.
- De SED stelt een tactisch informatiebeveiligingsbeleid op, stemt het beleid van de gemeenten en de SED op elkaar af en stelt ieder jaar een informatiebeveiligingsplan op, op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Het informatiebeveiligingsbeleid vormt samen met het jaarlijkse informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed, Gemeente en SED, benaderd.
- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisaties. Deze periodieke controle bestaat, onder andere, uit een jaarlijkse rapportage volgens de ENSIA systematiek.
- Informatiebeveiliging is een continu verbeterproces. De 'Plan, do, check en act'-cyclus vormt het managementsysteem van informatiebeveiliging.
- 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 en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast (IBBeleid Gemeente).
- Het AB van de SED stelt het tactisch informatiebeveiligingsbeleid SED (IBBeleid SED) vast.
- Het DB van de SED stelt jaarlijks het informatiebeveiligingsplan vast (IBPlan SED 20xx).
- De Directie van de SED is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op het IBBeleid Gemeente en IBBeleid SED in aanvullende beleidsdocumenten, regels en voorschriften. Van de 10 principes van informatiebeveiliging (zie onder 2.2.2) zijn de eerste 9 gemandateerd aan de SED.
- Het DB van de SED faciliteert het college door het voorzien in de noodzakelijke informatievoorziening ten behoeve van de 10e taak ('het bestuur controleert en evalueert')
- De Directie SED is verantwoordelijk voor het vragen om informatie bij de afdelingsleidinggevenden en ziet erop toe dat de afdelingsleidinggevenden adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) SED ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het AB/DB en aan de Directie, voorafgaand aan de P&C-gesprekken.

- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging naar aanleiding van de rapportage van de CISO SED. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- Leidinggevenden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT en 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 worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Leidinggevenden 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 prioritering van beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Leidinggevenden voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.
- De status van de maatregelen beschreven in de BIO wordt bijgehouden in een Information Security Management System (ISMS) waar de verantwoordelijke in de gemeente toegang toe heeft.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met alle ketenpartners in alle vormen van dienstverlening.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie worden actief bevorderd en geborgd.
- Periodiek wordt een informatiebeveiligingsplan (IB-Plan SED 20xx) opgesteld onder leiding van de Directie SED. Dit plan wordt afgestemd met de verantwoordelijke in de gemeente en is, onder andere, gebaseerd op:
 - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
 - Het dreigingsbeeld gemeenten van de IBD;
 - De door de leidinggevenden ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn;
 - Advies van informatiebeveiligingsmedewerkers van de gemeente, de SED en ketenpartners.

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 management verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officers) ondersteunt, adviseert, coördineert, bewaakt en rapporteert 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.

3.1 Organisatie

De verantwoordelijkheid voor de informatiebeveiliging ligt bij het College van B en W. De gemeente heeft alle uitvoerende taken gemandateerd aan de SED..

3.2 Sturingsschema

De sturing van de informatiebeveiliging is, vanwege de complexe structuur van de gemeente en de SED, verdeeld in meerdere delen:

Het college stelt het informatiebeveiligingsbeleid op strategisch niveau vast (dit beleid). Dit beleid vormt de kaders voor het informatiebeveiligingsbeleid op tactisch niveau.

Het AB van de SED stelt het informatiebeveiligingsbeleid op tactisch niveau vast. Hierin wordt het informatiebeveiligingsbeleid geconcretiseerd naar een praktisch niveau dat in de vorm van operationele maatregelen uitgevoerd wordt. De Directie SED is verantwoordelijk voor de uitvoering van het IB-Beleid SED.

Jaarlijks wordt een informatiebeveiligingsplan (IB-Plan) vastgesteld door het DB van de SED waarin de prioritering van de uit te voeren maatregelen vastgesteld wordt.

Vanuit de SED worden rapportages betreffende het informatiebeveiligingsbeleid samengesteld en regulier voorgelegd aan de directie SED, het AB/DB SED en het college. In ieder geval wordt de jaarlijkse ENSIA rapportage procedure doorlopen. Mogelijk dat de rapportages aanleiding geven tot bijstelling van het beleid. Op deze manier wordt de sturingscyclus gesloten.

3.3 Aansturing: Directie SED

De Directie SED zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een leidinggevende. De Directie SED zorgt dat de leidinggevenden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De Directie SED zorgt dat de CISO de Directie SED en het AB/DB SED informeert over de status van de informatiebeveiliging. Vanuit het DB SED worden de portefeuillehouders in de colleges geïnformeerd.

De Directie SED stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De Directie SED draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO SED. De Directie SED autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp

informatiebeveiliging wordt in de gemeenten en de SED gezien als een integraal onderdeel van risicomanagement.

3.4 Uitvoering: Leidinggevenden

Informatiebeveiliging valt onder de verantwoordelijkheden van alle leidinggevenden op alle niveau's, die hierin ondersteund 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 één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Leidinggevenden rapporteren aan de Directie 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 bedrijfsvoeringsoverleg.

Taken van de leidinggevenden 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.

Vorbereiding en coördinatie van het overleg ligt bij de CISO.

3.5 Uitvoering: CISO

De Chief Information Security Officer (CISO) is verantwoordelijk de ondersteuning, advisering, coördinering en bewaking van alle aspecten van de informatiebeveiliging, vanuit de SED maar voor de gemeente en de SED-organisatie gelijk.

De CISO bewaakt tevens of zowel de leidinggevenden van afdelingen als de leiding van de organisaties de verantwoordelijkheden op het gebied van de informatiebeveiliging nemen. De CISO wordt daartoe ten minste tweemaal per jaar bij het bedrijfsvoeringsoverleg uitgenodigd.

De CISO zorgt ervoor dat het ISMS operationeel blijft, zorgt ervoor dat activiteiten, welke worden aangegeven door het ISMS, op tijd starten en ondersteunt deze activiteiten met raad en daad.

De CISO zorgt voor de nodige controles, risicoanalyses en rapportages. De CISO rapporteert tenminste jaarlijks aan de Directie SED en het AB/DB SED en indien de status van de informatiebeveiliging daar aanleiding toe geeft. De CISO zorgt voor extra rapportages en uitleg aan de portefeuillehouders indien noodzakelijk.

De CISO zorgt ervoor dat het beleid van de gemeente en van de SED aan blijft sluiten bij de realiteit. Het jaarlijks vast te stellen IBPlan wordt voorbereid door de CISO.

Om de taken goed uit te kunnen voeren rapporteert de CISO rechtstreeks aan de Directie SED en het AB/DB SED waarbij de CISO een onafhankelijke positie kan innemen.

3.6 Controle en verantwoording

3.6.1 Jaarlijkse cyclus

Dit Strategisch Beleid is een verantwoordelijkheid van het College van de gemeente, de uitvoering op tactisch en operationeel niveau de verantwoordelijkheid van de SED.

De Directie SED is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiligingsaspecten aan het DB van de SED, in de praktijk verzorgt de CISO dit.

De Directie SED rapporteert jaarlijks over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid aan het DB SED. Deze jaarlijkse rapportage informatiebeveiliging wordt, na goedkeuring door het AB, doorgestuurd aan de colleges van de gemeenten.

De jaarlijkse rapportage, die door het college wordt ontvangen, wordt door het college via een collegebesluit ter kennis gebracht aan de raad. Door dat collegebesluit stemt het college in met het handelen van de SED.

De jaarlijkse rapportage en het collegebesluit volgt de ENSIA-systematiek maar wordt, indien noodzakelijk, uitgebreid met actuele onderwerpen.

3.6.2 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dat betekent dat jaarlijks de rol van ENSIA-coördinator wordt belegd bij de CISO, tenzij er redenen zijn om een ander aan te wijzen. De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke leidinggevenden. De leidinggevenden leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging komt tot uitdrukking in de Collegeverklaring Informatiebeveiliging, welke de CISO voorbereidt. 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.

