gemeente Stichtse Vecht

Beleid

Informatiebeveiligingsbeleid 2020 - 2023

INFORMATIEBEVEILIGINGSBELEID 2020-2023

AUTEUR(S):

S. Nagtegaal (Ciso)

DATUM	10 maart 2020
STATUS	Defintief
VERSIE	1.0

VERSIEBEHEER

Versie	Datum	Auteur	Opmerking
0.1	08-01-2020	S. Nagtegaal	Initiële opzet
0.2	15-01-2020	S. Nagtegaal	Aanpassing tekst
0.3	21-01-2020	S. Nagtegaal	Aanpassing tekst
0.4	03-02-2020	S. Nagtegaal	Aanvullingen en aanpassingen na meelezen
0.5	12-02-2020	S. Nagtegaal	Aanpassing tekst
0.6	18-02-2020	S. Nagtegaal	Aanpassing tekst
0.7	20-02-2020	S. Nagtegaal	Aanpassing tekst
1.0	09-03-2020	S. Nagtegaal	Besproken met programmanager

VASTSTELLING

Versie	Datum	Door	Vindplaats
1.0	18-03-2020	Directie	Samen@work bij Informatiebeveiligings- privacybeleid

MANAGEMENTSAMENVATTING

Voor u ligt het informatiebeveiligingsbeleid 2020-2023 van de gemeente Stichtse Vecht. In dit beleid worden de kaders gesteld waarbinnen, op het gebied van informatiebeveiliging, gewerkt moet worden.

Het doel is om in control te zijn met het beveiligen van (persoons)informatie waarmee binnen gemeente Stichtse Vecht wordt gewerkt en waarvoor de gemeente verantwoordelijk is. Het in control zijn en blijven op het gebied van informatiebeveiliging is een traject waar al een aantal jaren hard aan wordt gewerkt. Het goed omgaan met informatie is een taak van alle medewerkers van de gemeente, iedereen heeft hier een verantwoordelijkheid in.

Het informatiebeveiligingsbeleid houdt rekening met:

- De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- De Baseline Informatiebeveiliging Overheid (BIO)
- Het jaarlijks opgestelde dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
- Eisen die voortkomen uit van toepassing zijnde wet- en regelgeving
- Informatie uit incidenten, inbreuken op de beveiliging en bevindingen uit de Pentest

Dit beleidsstuk is de kapstok voor alle te nemen maatregelen en onderliggende beleidsstukken, processen en procedures op het gebied van informatiebeveiliging en wordt jaarlijks geëvalueerd. De maatregelen worden jaarlijks in de vorm van de Jaaropdracht Gegevensbescherming en Informatieveiligheid met concrete acties uitgewerkt en vervolgens uitgevoerd. Bij significante wijzigingen wordt het beleid aangepast.

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van Burgemeester en Wethouders. Vanaf dat moment vervangt het vastgestelde informatiebeveiligingsbeleid van 12 maart 2015.

Aldus vastgesteld door burgemeester en wethouders van gemeente Stichtse Vecht op 19 mei 2020.

De secretaris, De burgemeester,

drs. F.J. Halsema drs. A.J.H.T.H. Reinders

INHOUDSOPGAVE

1 INLEIDING

1.1 Aanleiding tot informatiebeveiliging

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot 2023 en vervangt het in 2015 vastgestelde Informatiebeveiligingsbeleid. 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 2020-2023' 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). De principes zijn gebaseerd op de 10 principes[1] voor informatiebeveiliging zoals uitgewerkt door de VNG.

1.2 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet en bevat de basisprincipes voor informatiebeveiliging. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.3 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.

- Beschikbaarheid: Het zorgdragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
- Integriteit: het waarborgen van de juistheid, volledigheid, en controleerbaarheid van informatie en informatieverwerking.
- Vertrouwelijkheid: de mate waarin informatie alleen toegankelijk is of wordt gemaakt voor degenen die hiervoor gerechtigd zijn.

[1] De 10 bestuurlijke principes voor informatiebeveiliging'. https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

1.4 Ambitie en visie van de gemeente op het gebied van informatiebeveiliging

De gemeente Stichtse Vecht is jong, nieuwsgierig, creatief, ondernemend en altijd in beweging. Want wat vandaag is, kan morgen anders zijn. Door samen te werken met inwoners en partners, en door de kracht van onze kernen als bron van initiatieven samen te brengen, kunnen we plannen voor de toekomst verwezenlijken. Om zo doeltreffend en flexibel mogelijk te zijn werken wij als gemeente wisselend in rol, en als organisatie in vrij laten waar kan en controle waar moet. Hierdoor zijn we wendbaar om bij iedere opgave te doen wat nodig is. De wereld om ons heen is continu in beweging en verandert steeds sneller. Hiermee is alles wat we doen voor onze inwoners en bedrijven.

De visie voor informatiebeveiliging is niet anders. Informatie is één van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.
Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren. Binnen de eigen organisatie, maar ook daarbuiten: met inwoners, ondernemers, ketenpartners en medeoverheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners verbeteren en meer mensen aan het werk krijgen. Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid hebben om de gegevens van hun inwoners onder alle omstandigheden te beschermen. Zorgvuldige omgang van de gemeente met informatie is het uitgangspunt. Dat vergt dat onze systemen goed beveiligd zijn en minimaal voldoen aan de geldende normen.

Informatiebeveiliging is een proces waarbij het continue leren op de eerste plaats staat en is ook niet bedoeld voor het winnen op de korte termijn. Het is een lange termijn strategie met vallen en opstaan. Dat vergt een nieuwe mind-set en maakt dat het onderwerp informatieveiligheid een vast onderdeel moet gaan worden op de bestuurstafel.

1.5 Geldigheid en evaluatie

Het informatiebeveiligingsbeleid heeft na vaststelling een geldigheidsduur van maximaal drie jaar en wordt jaarlijks geëvalueerd. Bij belangrijke wijzigingen van bijvoorbeeld landelijke wet- en regelgeving zal het beleidsstuk worden aangepast.

2 STRATEGISCH BELEID

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2020 tot 2023. De uitwerking van dit beleid in concrete maatregelen vindt plaats in de Jaaropdracht Gegevensbescherming en Informatieveiligheid.

2.2 Ontwikkelingen

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

2.2.1 De Baseline Informatiebeveiliging Overheid (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 Baseline Informatiebeveiliging Gemeente (BIG). Dat wil zeggen dat de teammanagers 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. Informatieveiligheid dient dus vanuit het primaire proces gestuurd te worden, daar waar het eigenaarschap van de informatie ligt. De teammanager kent het te beveiligen informatiesysteem en de te beschermen informatie uiteindelijk het best.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader [2] 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.

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

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

2.2.4 Informatie uit incidenten, inbreuken op de beveiliging en bevindingen uit de Pentest

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. Ook laat de gemeente, om kwetsbaarheden op te sporen en de digitale weerbaarheid te vergroten, jaarlijks een pentest uitvoeren. Dit heeft als doel om inzicht te krijgen in de status en effectiviteit van de beveiligingsmaatregelen.

2.2.5 Wetgeving

Wetgeving is aan verandering onderhevig en dat kan inhouden dat er wetswijzigingen zijn die tot gevolg hebben dat het gemeentelijk informatiebeveiligingsbeleid moet veranderen. Voorbeelden (niet uitputtend) hiervan zijn o.a. :

- Algemene Verordening Gegevensbescherming (AVG).
- Basis Registratie Personen (BRP).
- Basisregistratie Adressen en Gebouwen (BAG).
- Basisregistratie Grootschalige Topografie (BGT).
- Basisregistratie Ondergrond (BRO).
- Paspoortuitvoerregeling Nederland 2001 (PUN).
- Archiefwet 1995

2.3 Standaarden van 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[3] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende Basis Beveiligings Niveaus (BBN).

BBN 1
- Minimale beveiligings niveau voor overheidssystemen.
- Basisniveau en verplichte controls en maatregelen o.b.v. wet-& regelgeving (AVG) en beveiligingspricipes (uit de BIO).
- Beschikbaarheid Laag, Integriteit Laag, Vertrouwelijkheid Laag.

BBN 2
- Uitgangspunt voor gemeenten.
- Vertrouwelijke informatie, incidenten kunnen leiden tot bestuurlijke commotie, veiligheid van andere systemen wordt beïnvloed.
- Beschikbaarheid Midden, Integriteit Midden, Vertrouwelijkheid Midden.

BBN 3
- Weerstand tegen statelijke actoren, niveau AIVD, aanvullende maatregelen o.b.v. risicoanalyse.
- Alleen bij zeer grote impact, kritieke infrastructuur, staatsgeheimen.
- Beschikbaarheid Midden, Integriteit Midden, Vertrouwelijkheid Hoog.

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 Jaaropdracht Gegevensbescherming en Informatieveiligheid.

2.5 Scope informatiebeveiliging

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

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

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, PNIK en SUWI[4]. 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 limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

Het bestuur, de directie en de teammanagers 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 heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het 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. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Risicomanagement

De gemeente volgt een aanpak van informatieveiligheid op basis van risicobeheersing. Het streven naar 100% veiligheid is niet het uitgangspunt, het uitgangspunt is optimale beveiliging van informatie. Het richt zich op de bescherming van informatie tegen bedreigingen en gaat in principe uit van de beantwoording van drie vragen:

1. Wat zijn voor ons de meest waardevolle processen, informatiesystemen en informatie?
2. Welke gebeurtenissen kunnen schade toebrengen aan deze waardevolle informatiesystemen en informatie?
3. Wat doen we wel en vooral ook niet om deze informatiesystemen en informatie te beschermen tegen deze gebeurtenissen?

Het informatiebeveiligingsrisico is de som van de kans op een beveiligingsincidenten en de impact daarvan: **risico = kans x impact**. Risicomanagement is een gestructureerde manier om risico's en

[4] BRP is de Basis Registratie Personen, PNIK is Paspoort en Nederlandse Identiteitskaarten, SUWI is Structuur Uitvoeringsorganisatie Werk en Inkomen

gevolgen in kaart te brengen, te evalueren en pro-actief te beheersen door het treffen van maatregelen. Met een aanpak gebaseerd op risicobeheersing is de gemeente beter in staat om een evenwichtige set van veiligheidsmaatregelen te implementeren en om daarbij een betere afweging tussen kosten en noodzaak te maken. Dit zorgt ervoor dat informatiebeveiliging zo optimaal mogelijk ingericht kan worden. Minder maatregelen en meer focus leggen op grote risico's.

2.6.2 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.

2.6.3 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 de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijn management. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Stichtse Vecht 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 de Jaaropdracht Gegevensbescherming en Informatieveiligheid het fundament onder een betrouwbare informatievoorziening. In de Jaaropdracht Gegevensbescherming en Informatieveiligheid wordt de betrouwbaarheid van de informatievoorziening organisatiebreed 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 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.
- Continuïteit, bij continuïteitsbeheer gaat het om maatregelen die gericht zijn om langdurige onderbreking van bedrijfsactiviteiten bij de gemeente tegen te gaan en om kritische bedrijfsprocessen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
- Security by design, security maakt onderdeel uit van de processen en dient vanaf de beginfase betrokken te zijn.

2.6.4 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch Informatiebeveiligings-beleid vast.
- De directie stelt jaarlijks de Jaaropdracht Gegevensbescherming en Informatieveiligheid vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie , 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, kunnen worden opgenomen in de auditplannen.
- De teammanagers 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 die voor hen van toepassing zijn.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Teammanagers 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. Teammanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.5 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 (bewustwording).
- Jaarlijks wordt de Jaaropdracht Gegevensbescherming en Informatieveiligheid opgesteld door het Privacy Informatieveiligheid Team (PIT), gebaseerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA).
  - het dreigingsbeeld gemeenten van de IBD.
  - informatie uit incidenten, inbreuken op de beveiliging en bevindingen uit de Pentest
  - De door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3 ORGANISATIE, TAKEN & VERANTWOORDELIJKHEDEN

3.1 Doel

Informatiebeveiliging vereist een governance structuur waarin rollen en verantwoordelijkheden op het gebied van Informatiebeveiliging zijn gedefinieerd. 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, PO en FG) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering. Informatiebeveiliging is de verantwoordelijkheid van iedereen die voor de gemeente werkt. Onderstaand zijn een aantal rollen en verantwoordelijkheden verder uitgewerkt. Het is voornamelijk van belang de relatie tussen de verschillende rollen te verhelderen.

3.2 Het College van B&W en de gemeenteraad

Het College van B&W stelt formeel het informatiebeveiligingsbeleid vast en is bestuurlijk verantwoordelijk voor informatiebeveiliging binnen de gemeente. Een van de wethouders is de portefeuillehouder en is daarmee ook eindverantwoordelijk voor het goed beveiligen van de gemeentelijke informatie. Door middel van het hoofdstuk informatieveiligheid in het jaarverslag en de uitkomsten van ENSIA in de collegeverklaring legt het College verantwoording af aan de gemeenteraad over informatieveiligheid.

3.3 Directieteam

De gemeentesecretaris is binnen de gemeente ambtelijk eindverantwoordelijk voor de informatiebeveiliging. De directie belegt alle processen en systemen en de daarbij behorende middelen onder de verantwoordelijkheid van de teammanagers. De directie zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie binnen hun scope. De directie 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.

De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. BBN 2 is het uitgangspunt voor gemeenten. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de gemeente Stichtse Vecht gezien als een integraal onderdeel van risicomanagement.

3.4 Teammanagers

Informatiebeveiliging valt onder de verantwoordelijkheid van de teammanager. 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. Teammanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in de directieraad.

Taken van de teammanagers 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. Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.5 Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) is verantwoordelijk voor de organisatie van informatiebeveiliging. De CISO heeft als taak informatieveiligheid op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelfverantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. Daarbij rapporteert de CISO periodiek over de gang van zaken. Onderstaand een aantal taken van de CISO ten aanzien van informatiebeveiliging:

- Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen.
- Ondersteunt management bij het opstellen van informatiebeveiligingsrapportages en beoordeelt deze rapportages.
- Periodiek rapporteren over de voortgang van de planning, status van informatiebeveiliging, incidenten en andere ontwikkelingen aan de portefeuillehouder.
- Het inrichten van de informatiebeveiligingsorganisatie.
- Het uitvoeren van informatiebeveiligingsassessments.
- Het toezien op naleving van de eisen voor informatiebeveiliging.
- Het bevorderen van het informatiebeveiligingsbewustzijn over de hele organisatie.
- De voorbereiding op toekomstige informatiebeveiligingsrisico’s en ICT-beveiligingsrisico’s o.b.v. het dreigingsbeeld Nederlandse Gemeenten.
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten.

3.6 Functionaris Gegevensbescherming (FG)

De Functionaris Gegevensbescherming (FG) is ingesteld op grond van de Algemene Verordening Gegevensbescherming (AVG). De FG is een onafhankelijke toezichthouder met als hoofdtaak: er op toezien dat de gemeente de aan haar toevertrouwde persoonsgegevens in voldoende mate beschermt en beveiligt volgens de normen van de AVG. De taken van de FG zijn terug te vinden in de relevante artikelen uit de AVG en zijn onder andere:

- informeren en adviseren over privacywet- en regelgeving;
- toezien op de naleving van privacywet- en -regelgeving, inclusief het interne privacybeleid;
- adviseren over en toezien op de uitvoering van Data Privacy Impact Assessments (DPIA's);
- fungeren als aanspreekpunt voor betrokkenen;
- optreden als aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

3.7 Privacy Officer (PO)

De Privacy Officer houdt zich dagelijks bezig met de uitvoering van het privacybeleid. De Privacy Officer brengt de verwerkingen van persoonsgegevens en de privacyrisico's hiervan in kaart, beoordeelt verwerkersovereenkomsten en convenanten over gegevensuitwisseling af en heeft een adviserende rol richting de organisatie. Ook neemt de Privacy Officer, samen met de FG en de CISO, deel aan het Privacy Informatiebeveiliging Team (PIT). Het PIT komt bijeen bij een datalek en neemt maatregelen om deze te dichten en schade te voorkomen en te beperken. De CISO, PO en FG werken nauw met elkaar samen.

3.8 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente Stichtse Vecht. De bestuurders en directie zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie. De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.8.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Deze zelfevaluatie wordt gedaan aan de hand van de Eenduidige Normatiek Single Information Audit (ENSIA). De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de afdeling waar de vraag betrekking op heeft. Op die manier wordt men op de afdelingen bewust dat zij hierin ook een verantwoordelijkheid hebben.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking en 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 worden het bestuur van de gemeente Stichtse Vecht en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.