Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Datum
26 november 2025
Versie
Definitief
Auteur(s)
Danielle Huijdts, Juliette Mies en Peter van Enk

Digitale Veiligheid in Stichtse Vecht

Huis Op Orde in de aanloop naar de Cyberbeveiligingswet

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Colofon

De Rekenkamer van de gemeente Stichtse Vecht bestaat uit drie externe leden en wordt ondersteund door een ambtelijk secretaris.

Leden Rekenkamer: Martijn Bakker (voorzitter), Robert Olieman, Kirsten van Steenbergen

Secretaris: Jacqueline Willenborg

Uitvoerend bureau: PBLQ (Peter van Enk, Danielle Huijdts, Juliette Mies)

Postadres: Rekenkamer Stichtse Vecht, Postbus 1212, 3600 BE Maarssen

e-mail: rekenkamer@stichtsevecht.nl

telefoon: 0346-254200

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Inhoudsopgave

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Conclusies en aanbevelingen

De gemeente Stichtse Vecht is (net als alle andere gemeenten) steeds digitaler gaan werken. Er is geen gemeentelijk proces meer zonder digitale component. Daarom is ook informatiebeveiliging steeds belangrijker; een digitale verstoring kan niet alleen gevolgen hebben voor de gemeentelijke dienstverlening, als persoonsgegevens van inwoners op straat komen te liggen, gaat dit ook ten koste van het vertrouwen van de inwoners.

Het veranderende wettelijk kader onderstreept het belang van informatiebeveiliging voor overheden. De Europese NIS2-richtlijn en de nationale vertaling, de Cyberbeveiligingswet (Cbw), stellen extra eisen aan gemeenten. De Cbw treedt naar verwachting in het tweede kwartaal van 2026 in werking. De rekenkamer Stichtse Vecht voert, vooruitlopend hierop, een onderzoek uit naar de wijze waarop de gemeente zich hierop heeft voorbereid. Hierbij wordt speciaal aandacht besteed aan de rol van de gemeenteraad.

Conclusies

Digitale infrastructuur
Uit het onderzoek is allereerst naar voren gekomen dat de gemeente Stichtse Vecht van ver komt en bezig is met een inhaalslag op het gebied van digitalisering. Een belangrijk onderdeel hiervan betreft de gemeentelijke digitale infrastructuur. Een aantal jaren geleden had de gemeente nog een eigen ‘serverpark’ waarop de gemeentelijke applicaties draaiden en was de gemeente zelf verantwoordelijk voor het technisch beheer van zowel hard- als software. Inmiddels zijn en worden applicaties overgebracht naar ‘de cloud.’ Daarmee zijn leveranciers voor een belangrijk deel verantwoordelijk voor de uitvoering van de technische informatiebeveiliging. Het blijft echter een verantwoordelijkheid van de gemeente zelf om aan de wettelijke beveiligingseisen en -normen te voldoen.

Beleid en uitvoering
In het ‘Strategisch beveiligingsbeleid 2020 - 2023’ is vastgelegd volgens welke kaders Stichtse Vecht haar informatieveiligheid inricht. Vanwege op handen zijnde Cbw is besloten om na 2023 geen nieuw beleid op te stellen, maar de houdbaarheid van het beleid te verlengen. Het plan doet enigszins gedateerd aan en recente ontwikkelingen (wetgeving, normenkaders en toegenomen bedreigingen) zijn er niet in meegenomen.

Het strategisch beleidsdocument is gebaseerd op een format van de Informatiebeveiligingsdienst (IBD) van de VNG. Dit heeft als voordeel dat belangrijke zaken op het gebied van informatiebeveiliging onderdeel zijn van het beleid. Echter er wordt in de praktijk niet altijd conform dit beleidsdocument gewerkt. De afwijkingen tussen beleid en praktijk is op een aantal zaken significant. In het beleidsdocument wordt gesproken over de Baseline Informatiebeveiliging Overheid (BIO) als (het nieuwe) normenkader voor de gehele overheid. De BIO is de baseline voor informatiebeveiliging en is dus de ‘ondergrens’. Stichtse Vecht voldoet niet aan deze ondergrens, zo blijkt uit de zelfevaluaties die gehouden zijn in 2021, 2023 en 2024. In dat laatste jaar haalt de gemeente 73% van de norm (dat is lager dan het jaar daarvoor). Dit zorgt voor kwetsbaarheden en verhoogt het risico op digitale verstoringen.

Als aanvulling op de BIO zijn er in het strategisch beleid 10 principes voor informatiebeveiliging benoemd. Aan de principes die betrekking hebben op risicomanagement (Informatiebeveiliging is risicomanagement en Risicomanagement is onderdeel van de besluitvorming) wordt niet voldaan. Ook het 10de en laatste principe over de rol van het bestuur (het bestuur controleert en evalueert) zien wij onvoldoende terug.

In het strategisch beleid is vastgelegd dat: ‘het beleid zal worden uitgewerkt in tactisch en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

uitgewerkt in het jaarlijks te schrijven Jaaropdracht Gegevensbescherming en Informatieveiligheid.' Deze jaaropdracht en de bijbehorende bestuurlijke rapportage wordt niet structureel geleverd. Alleen voor 2022 is een Jaaropdracht aangetroffen en de onderzoekers hebben een bestuurlijke rapportage over 2021 ontvangen.

Ook aan een ander belangrijk uitgangspunt uit het beleid, de 'Plan Do Check Act cyclus, wordt niet voldaan. Er is op dit moment geen effectieve verbetercyclus, zo schetst ook de gemeente zelf in een 'Verkenning Digitale Weerbaarheid'. In dit document worden daarnaast scenario's geschetst om te voldoen aan de wettelijke normen en wel een effectieve verbetercyclus in te richten. Ook wordt een scenario geschetst om de werkwijze van het eigen strategisch beleid te volgen en te voldoen aan de extra eisen van de Cbw.

In de interviews worden twee belangrijke oorzaken aangedragen voor het feit dat er niet volgens het eigen beleid gewerkt wordt. De eerste is de bovengenoemde inhaalslag inclusief de migratie naar 'de Cloud'. De tweede oorzaak is het huidige gebrek aan ambtelijke capaciteit.

Er gaat ook een aantal zaken wel goed. Zo zijn medewerkers zich goed bewust van het belang van informatiebeveiliging. Zij weten bij vragen de CISO en de FG goed te vinden. Ook op technisch vlak is er, als onderdeel van de eerder genoemde inhaalslag, veel aandacht voor informatiebeveiliging. Dat blijkt onder andere uit controle die is uitgevoerd bij de ICT-leveranciers die betrokken zijn bij de belangrijkste processen van Stichtse Vecht. Bovendien zijn de extra eisen die de Cbw aan de gemeenten stelt goed in beeld, niet alleen voor wat betreft de gewenste eindsituatie, maar ook voor wat betreft mensen, middelen en activiteiten.

De rol van het bestuur
De rol van het bestuur verandert dus onder de Cbw. In de Cyberbeveiligingswet en onderliggende Algemene maatregelen van Bestuur (AmvB) is de rol van het college van B&W verankerd. Het College wordt verplicht om, met kennis van zaken, risicogericht te sturen op informatiebeveiliging. Het College wordt verplicht om een training te volgen en de toezichthouder (de Rijksdienst Digitale Infrastructuur) kan bestuurders een boete opleggen als zij dit niet doen.

Deze verandering geldt ook voor Stichtse Vecht. Op dit moment wordt de portefeuillehouder in het college van B&W eens in de twee maanden bijgepraat over recente ontwikkelingen en heeft de bestuurder veel vertrouwen in de kwaliteit van zijn ambtelijke organisatie. Er wordt niet periodiek gerapporteerd over de staat van de uitvoering en ontwikkelingen in het dreigingsbeeld aan het college. Wij hebben daarom ook niet vast kunnen stellen dat besluitvorming over informatiebeveiliging gebaseerd is op risicomanagement. Dat betekent dat de sturing op dit moment niet aan de eisen van de Cbw voldoet.

Datzelfde geldt voor de gemeenteraad, die op dit moment het college van B&W onvoldoende controleert en niet in staat is om (financiële en inhoudelijke) kaders te stellen. In de raadssessie die in het kader van dit onderzoek heeft plaatsgevonden, geven raadsleden aan dat informatiebeveiliging net als bijvoorbeeld Jeugdzorg als een volwaardig gemeentelijk domein beschouwd zou moeten worden. Raadsleden zeggen niet over een sturingskader te beschikken, waardoor zij naast hun controlerende rol ook hun kaderstellende rol onvoldoende kunnen waarmaken.

Aanbevelingen

Bovenstaande conclusies leiden tot de volgende aanbevelingen:

1. **Vraag het college om een passend strategisch beleid voor informatiebeveiliging**

Het huidige strategisch informatiebeveiligingsbeleid is dringend aan vernieuwing toe. Hiermee is gewacht omdat de Cyberbeveiligingswet nog onbekende verplichtingen voor gemeenten met zich

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

zou meebrengen. Ondanks het feit dat de inwerkingtreding van de Cbw is uitgesteld tot het tweede kwartaal van 2026 is er al voldoende duidelijkheid om het beleidskader te vernieuwen.

Gezien de Cbw-verplichting van risicogerichte sturing door het College, is het van belang dat er in het beleidskader voldoende aandacht wordt besteed aan de rol van het bestuur. Ook adviseren wij om het college te betrekken bij de voorbereiding op het beleidskader. Bij de invulling van het beleidskader kan gebruik gemaakt worden van formats die door de Informatiebeveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG) beschikbaar gesteld worden.

2. **Zorg voor voldoende capaciteit (mensen en middelen) en ambtelijke prioriteit om conform het nieuwe strategisch beleid te werken en aan de wettelijke verplichtingen te voldoen.**

Ambtelijk heeft men goed in beeld wat er in praktijk moet gebeuren om aan de veranderende wettelijke kaders en vigerende normen te voldoen. Er is namelijk gedetailleerd beschreven wat hiervoor aan (extra) mensen en middelen nodig is. Als deze informatie geagendeerd wordt in de gemeenteraad kan die invulling geven aan zijn kaderstellende rol,

3. **Vraag het college om de raad op korte termijn te informeren over de bestuurlijke risico-afwegingen die de gemeente neemt**

De sturing door het college van B&W is op dit moment onvoldoende. Het college is zich op dit moment niet bewust van het feit dat de gemeente niet aan de geldende BIO-norm voldoet en welke risico's dat met zich meebrengt. Dat komt voor een belangrijk deel doordat er niet periodiek gerapporteerd wordt. Wij bevelen daarom aan om het bestuur periodiek te rapporteren over de stand van zaken ten aanzien van informatiebeveiliging. In deze rapportage zou, vooruitlopend op de Cbw, aandacht moeten zijn voor risicomanagement. Voor deze bestuurlijke rapportage kan gebruik gemaakt worden van het bestaande formats die voor alle gemeenten beschikbaar zijn in het ENSIA platform.

4. **Maak afspraken met het college over welke informatie de gemeenteraad periodiek nodig heeft om te kunnen sturen en controleren.**

De informatie die de raad ontvangt in de P&C-cyclus met betrekking tot het onderwerp digitale veiligheid is onvoldoende om de controlerende en kaderstellende rol waar te kunnen maken. Mede op basis van de raadsbijeenkomst bevelen wij aan om de raad periodiek te informeren over de mate waarin de gemeente aan de geldende normen- en toezichtskaders voldoet. Deze kaders zijn vastgelegd in de BIO (die wordt doorontwikkeld naar de BIO2) en de kaders van verschillende stelselhouders. Ook zou de raadsinformatie informatie moeten bevatten over het resultaat van het risicomanagement door het college van B&W. Ook voor de rapportage aan de gemeenteraad is in het ENSIA platform een format beschikbaar.

Aan de rapportage aan het college van B&W en de gemeenteraad moet een effectieve PDCA-cyclus ten grondslag liggen.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

1. Inleiding

1.1. Aanleiding voor het onderzoek

Gemeenten inventariseren en beheren steeds meer informatie over hun inwoners. Veel van deze informatie raakt aan hun persoonlijke levenssfeer. Bovendien heeft de informatie vaak betrekking op mensen in een kwetsbare positie die afhankelijk zijn van gemeentelijke ondersteuning. Dat vraagt om extra garanties voor een veilige omgang met die informatie en een veilige inrichting van de onderliggende systemen.

Informatieveiligheid wordt steeds belangrijker door de toenemende digitalisering. Gemeenten verwerken naast persoonsgegevens veel andere belangrijke gegevens die goed beschermd moeten worden. Informatieveiligheid wordt nog vaak als een verantwoordelijkheid van de IT-afdeling gezien. Dit is een te beperkte insteek om voor een adequate bescherming van gemeentelijke informatie te zorgen. Van de baliemedewerker tot het gemeenteraadslid, allemaal spelen ze een rol als het gaat om digitale veiligheid. Informatieveiligheid zou een kernwaarde moeten zijn van iedere medewerker. De menselijke factor en de dagelijkse uitvoeringspraktijk in de gemeente is daarom een belangrijk aandachtspunt in dit onderzoek. Daarnaast is er aandacht voor de raad. Wordt de raad in staat gesteld om haar controlerende- en kaderstellende rol uit te voeren? Maar ook: geeft de raad voldoende prioriteit aan dit onderwerp?

Het laatste belangrijke deel van het speelveld betreft de weerbaarheid van de organisatie. 100% Digitaal veilig bestaat niet; de kans op een digitale verstoring is altijd aanwezig. De vraag is hoe de gemeente hierop is voorbereid. Weerbaarheid begint bij het bewustzijn van de medewerkers. Ook de adequate inrichting en reactie van de crisisorganisatie speelt een belangrijke rol in de responsfase van een digitale verstoring. In ons onderzoek hebben wij aandacht besteed aan beide zaken. Zo zijn wij in focusgroepen nagegaan hoe het met het bewustzijn van de medewerkers is gesteld. Ook hebben wij aandacht besteed aan de crisisorganisatie. Wij hebben hierbij niet alleen gekeken naar de inrichting en werkprocessen, maar ook naar cyberoefeningen. Worden deze uitgevoerd en wordt hiervan geleerd?

In het tweede kwartaal van 2026 wordt naar verwachting de Cyberbeveiligingswet van kracht. Gemeenten worden (net als andere overheidsorganisaties) gezien als essentiële entiteiten. Dit betekent dat er extra verplichtingen voor gemeenten gaan gelden op het gebied van de zorgplicht en de meldplicht. Deze wet is een directe aanleiding voor de Rekenkamer van Stichtse Vecht om dit onderzoek uit te voeren. Net als bij eerdere wetten met een grote impact op de gemeente (Omgevingswet en de decentralisaties binnen het Sociaal Domein), wil de Rekenkamer weten of de gemeentelijke organisatie goed voorbereid is. Ook wil de Rekenkamer met dit onderzoek de gemeenteraad nader informeren over dit belangrijke onderwerp, zodat de raad zijn kaderstellende en controlerende rol adequaat kan vervullen.

1.2. Probleemstelling en onderzoeksvragen

De Rekenkamer heeft onderzocht of de gemeente Stichtse Vecht goed voorbereid is op de Cyberbeveiligingswet en heeft daarbij de volgende onderzoeksvraag geformuleerd:

Is de informatieveiligheid bij de gemeente Stichtse Vecht voldoende gewaarborgd bij de invoering van de Cyberbeveiligingswet?

De onderzoeksvraag is beantwoord aan de hand van een aantal deelvragen. De deelvragen zijn hieronder per thema in een tabel opgenomen en worden elk in een separaat hoofdstuk beantwoord.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

	Deelvragen
Proces en organisatie (hoofdstuk 3)	**1. Wat doet de gemeente Stichtse Vecht op het gebied van informatieveiligheid?** • Welk beleid voert de gemeente op informatieveiligheid? • Heeft de gemeente nog aanvullende maatregelen benoemd buiten de 10 maatregelen die in de wet genoemd worden? • Welke risico's heeft de gemeente geïnventariseerd en welke beheersingsmaatregelen zijn daarbij benoemd? • In hoeverre zijn deze maatregelen geïmplementeerd? • Hoe communiceert de gemeente met betrokkenen en inwoners over datalekken?
Mens (hoofdstuk 4)	**2. Hoe bevordert de gemeente het bewust omgaan met informatie?** • Krijgen medewerkers voldoende uitleg en ondersteuning om veilig te werken? • Hoe gaan de medewerkers van de gemeente in de praktijk om met informatieveiligheid? • Hoe controleert de gemeente op het naleven van veilig werken en het voorkomen van informatiebeveiligingsincidenten en datalekken?
Techniek (hoofdstuk 5)	**3. Zijn gegevens bij de gemeente goed beschermd tegen de toegang door onbevoegden?** • Zo niet, Welke gevolgen heeft dit voor burgers en bedrijven? • Wat zijn de risico's en kwetsbaarheden? • Is het mogelijk om oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente in beheer heeft? • Welke penetratietesten voerde de gemeente uit? Zo ja, zijn verbeterplannen opgesteld naar aanleiding van de pentesten en zijn deze opgevolgd? • In hoeverre wordt in de organisatie vastgelegd wie wanneer toegang vraagt tot bestanden met gevoelige informatie (het loggen)? • Hoe is het autorisatiebeleid vorm gegeven en hoe wordt dit up to date gehouden?
Overige maatregelen (hoofdstuk 6)	**4. Welke (verdere) maatregelen zijn mogelijk om de informatieveiligheid te optimaliseren?** • Heeft de gemeente een beeld bij de extra verplichtingen uit de cyberbeveiligingswet (BIO2, Ensia2, meldplicht en toezicht)? • Zo ja, hoe bereidt de gemeente zich hierop voor?
Gemeenteraad (hoofdstuk 7)	**5. Hoe is de raad betrokken bij (de uitvoering van) het beleid ten aanzien van de informatieveiligheid?** • Wordt de gemeenteraad goed geïnformeerd over de risico's en maatregelen? • Welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook ingezet?

Op basis van deze hoofd- en deelvragen heeft de rekenkamer bij aanvang van het onderzoek een normenkader vastgesteld. Dit normenkader is opgenomen in bijlage D en voorzien van een stoplichtenrapportage. Hiermee geven wij op detailniveau aan aan welke normen de gemeente voldoet en aan welke normen niet.

1.3. Afbakening van het onderzoek

Uitgangspunt voor het onderzoek is het wettelijk kader. Hieronder valt de al genoemde Cyberbeveiligingswet, die bestaat uit drie hoofdonderdelen: zorgplicht, meldplicht en toezicht. De zorgplicht omvat maatregelen waarbij gemeenten verplicht zijn om risicoanalyses uit te voeren en passende maatregelen te nemen voor de beveiliging van hun netwerk- en informatiesystemen. Als onderdeel hiervan is gekeken in welke mate de gemeente voldoet aan de algemene Baseline

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Informatieveiligheid Overheid (BIO) en specifieke veiligheidsnormen van verschillende stelselhouders die opgenomen zijn in de Eenduidige Normatiek Single Information Audit (ENSIA).

1.4. Aanpak van het onderzoek

Om de onderzoeksvragen te beantwoorden zijn verschillende onderzoeksactiviteiten uitgevoerd. Allereerst is er een documentstudie uitgevoerd naar het beleid met betrekking tot informatieveiligheid, de inrichting van de technische beveiliging en de aandacht voor het veiligheidsbewustzijn. Vervolgens zijn interviews gehouden met sleutelpersonen zoals de portefeuillehouder in het college, de gemeentesecretaris, de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO), en andere functionarissen die betrokken zijn bij de digitale veiligheid.

In een focusgroep is geïnventariseerd in hoeverre er in verschillende beleidsdomeinen aandacht is voor informatieveiligheid. Er is nagegaan hoe de medewerkers van de gemeente in hun dagelijkse praktijk omgaan met informatieveiligheid, hoe ze hierin geschoold worden en hoe zij omgaan met hun taken en bevoegdheden. Speciale aandacht ging uit naar de borging door het management en de toegang tot CISO, FG en andere veiligheidsfunctionarissen. In de bijeenkomst is ook aandacht besteed aan de organisatiecultuur.

Daarnaast is er een bijeenkomst met de raad georganiseerd, waarin gekeken is hoe de raad de kaderstellende en controlerende rol op het gebied van digitale veiligheid invult. Niet de techniek, maar de (risico)sturing stond tijdens deze bijeenkomst centraal.

1.5. Leeswijzer

In het volgende hoofdstuk beschrijven wij de veranderende wettelijke context voor gemeentelijke informatieveiligheid. Hierbij vermijden wij technisch jargon en bieden wij de raadsleden van Stichtse Vecht handvatten voor sturing op dit domein. In de hoofdstukken 3 tot en met 7 beantwoorden we de deelvragen zoals hierboven beschreven.
In de bijlagen is het normenkader voor dit onderzoek opgenomen. Hierbij is, aan de hand van een stoplichtenrapportage aangegeven in welke mate Stichtse Vecht aan de normen voldoet. Ook bevatten de bijlagen een overzicht van bestudeerde documentatie en een overzicht van de gevoerde interviews.

gemeente Stichtse Vecht

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

2. Veranderende context gemeentelijke digitale veiligheid

2.1. Waarom is gemeentelijke digitale veiligheid belangrijk?

Digitale veiligheid gaat over veel meer dan bedrijfsvoering. De gemeentelijke dienstverlening is van digitalisering afhankelijk. Bovendien beschikken gemeenten over steeds meer persoonsgegevens van hun inwoners. Deze inwoners mogen van hun gemeente verwachten dat deze gegevens veilig zijn en dus niet op straat komen te liggen. Als dat toch gebeurt, dan schaadt dit het vertrouwen in de gemeentelijke overheid, en brengt mogelijk zelfs (directe) schade toe aan de getroffen inwoners.

Elke gemeente moet maatregelen nemen om ervoor te zorgen dat persoonsgegevens veilig zijn en de continuïteit van dienstverlening wordt geborgd. 100% Veilig bestaat echter niet; er is altijd een risico dat er iets misgaat, bijvoorbeeld dat een hacker inbreekt in een gemeentelijk informatiesysteem. Deze dreiging komt niet alleen van buiten, ook een slordigheidje van een van de eigen medewerkers kan leiden tot bijvoorbeeld een datalek.

Daarnaast is informatiebeveiliging ook vaak in het belang van de gemeente zelf, denk bijvoorbeeld aan informatie over voorbereidingen op strategische aankopen. Dergelijke informatie is niet per se door wetgeving beschermd, echter iedere gemeente realiseert zich dat dergelijke informatie niet moet lekken.

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 (persoons)gegevens en andere informatie.

In het algemeen leggen gemeenten hun doelstellingen, processen en rolverdeling vast in een beleidsdocument. Hierbij maken veel gemeenten gebruik van het format van de Informatiebeveiligingsdienst (IBD) van de VNG. Dit format gaat ervan uit dat een beleidsplan voor een periode van meestal vier jaar wordt vastgesteld. Op tactisch niveau wordt het beleid uitgewerkt in jaarplannen.

2.2. Wet- en regelgeving

Bij de uitvoering van het informatieveiligheidsbeleid moeten gemeenten voldoen aan verschillende wetten en regels. De belangrijkste zijn de Europese Network- and Information Security 2 directive (NIS2), de Cyberbeveiligingswet (Cbw), de Algemene Verordening Gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en de Eenduidige Normatiek Single Information Audit (ENSIA).

De NIS2-richtlijn van de Europese Unie heeft als doel om de informatiebeveiliging van essentiële diensten, waaronder die van gemeenten, in de EU-lidstaten te verbeteren. In de richtlijn is hiertoe onder meer een zorgplicht en een meldplicht opgenomen, en wordt ook het toezicht op informatiebeveiliging geregeld. De NIS2-richtlijn is niet rechtstreeks van toepassing op gemeenten, maar wordt uitgewerkt in de Cyberbeveiligingswet, waar gemeenten wel aan moeten voldoen. Bij aanvang van dit onderzoek was de verwachting dat de Cyberbeveiligingswet in oktober van dit jaar (2025) in werking zou treden. De wet lijkt nu uitgesteld tot het tweede kwartaal van 2026. Dat betekent geenszins dat de voorbereidingen die de gemeente treft c.q. getroffen heeft voor niets zijn geweest.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Vanaf het moment dat de wet ingaat, moet de gemeentelijke informatiebeveiliging voldoen aan de eisen van deze wet. De invoering van de Cyberbeveiligingswet leidt tot een taakverzwaring en extra kosten voor gemeenten. De VNG heeft in een reactie op deze wet gevraagd om compensatie van het Rijk voor deze kosten.[1]

De maatregelen die de Cyberbeveiligingswet voorschrijft om de informatiebeveiliging te verbeteren, de zorgplicht, zijn grotendeels opgenomen in de BIO2. In de Cyberbeveiligingswet gaat het naast de beveiliging van kantoorautomatisering (KA) ook over de beveiliging van operationele technologie (OT). Deze OT betreft bijvoorbeeld gemeentelijke bruggen en sluizen die op afstand worden bediend, en camera's in de openbare ruimte. Nieuw met de komst van de Cyberbeveiligingswet is ook dat er naast ad hoc toezicht (achteraf, via rapportage aan de raad en de stelselhouders bij het Rijk) ook proactief toezicht zal worden gehouden op de informatiebeveiliging van gemeenten. De Rijksinspectie Digitale Infrastructuur (RDI) is daarvoor aangewezen als toezichthouder voor de gemeenten en andere overheidsorganisaties.

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening betreft een uitwerking van Europese regelgeving die bedoeld is om de privacy van alle inwoners (beter) te beschermen. De Autoriteit Persoonsgegevens houdt toezicht op de uitvoering van de AVG in Nederland. Wanneer gemeenten de bescherming van persoonsgegevens niet op orde hebben, riskeren zij een boete van de Autoriteit Persoonsgegevens. Het maatschappelijk en financieel belang van een adequaat privacybeleid is groot. Gemeenten hebben echter niet alleen een goed privacybeleid nodig, maar ook een goede uitvoering daarvan. Beiden zijn verplicht op grond van de AVG. Omdat de beveiliging van persoonsgegevens veel raakvlak heeft met de beveiliging van informatie in het algemeen, zijn de verplichtingen die voortvloeien uit de AVG ook meegenomen in dit onderzoek.

De BIO is sinds 2019 het verplichte basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (en dus ook gemeenten). De BIO is gebaseerd op de informatiebeveiligingsstandaarden ISO 27001 en ISO 27002 en omvat een minimum aan maatregelen die getroffen moeten worden op het gebied van informatiebeveiliging. Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk in belangrijke mate op deze BIO. De BIO wordt op dit moment doorontwikkeld naar de BIO2 en wordt wettelijk verplicht onder de Cyberbeveiligingswet. In de BIO2 is mede naar aanleiding van de komst van de Cyberbeveiligingswet de verantwoordelijkheid van het hogere management in de gemeentelijke informatiebeveiliging vastgelegd. Ook het toewijzen van benodigde middelen, het verhogen van veiligheidsbewustzijn en het uitvoeren van controles maken onderdeel uit van de BIO2.

Voor raadsleden biedt de BIO aanknopingspunten om hun controlerende en kaderstellende rol in te vullen. De BIO kent vijf onderdelen die het hele domein van informatiebeveiliging goed afdekken:

BIO onderdeel	Toelichting
Beleid en organisatie	Actueel beleid en organisatie van informatiebeveiliging, bewustwording en (controle op) naleving
Personeel en toegang	Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens
Continuïteit en incidenten	Zorgen voor de continuïteit van de gemeentelijke dienstverlening en opvolging van incidenten
Informatiesystemen	Veilige omgang met informatiesystemen en afspraken hierover met leveranciers
Databescherming	Veilige omgang met data in gemeentelijke software

[1] zie VNG-reactie consultatie Cyberbeveiligingswet (NIS2) | VNG voor meer informatie

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Door de raad op hoofdlijnen inzicht te geven in de mate waarin de gemeente voldoet aan de BIO-normen, wordt duidelijk waar de informatiebeveiliging op orde is en waar nog een extra inzet gepleegd moet worden om aan het wettelijk kader te voldoen.

ENSIA is ontstaan uit een gezamenlijk initiatief van een aantal departementen en de VNG. Het doel van ENSIA is om tot een effectief en efficiënt ingericht verantwoordingsstelsel voor informatieveiligheid te komen. De ENSIA is een jaarlijkse audit die gebaseerd is op de BIO. Uitgangspunt voor ENSIA is het horizontale verantwoordingsproces waarin het college van B&W. zich over de informatieveiligheid verantwoordt aan de gemeenteraad. Deze verantwoording vormt de basis voor de verantwoording aan de stelselhouder (bijvoorbeeld het ministerie van BZK of SZW). Er wordt dus jaarlijks één audit uitgevoerd waarvan (een deel van) de resultaten zowel naar de gemeenteraad als de stelselhouder gaan. Net als de BIO, wordt ook de ENSIA op dit moment doorontwikkeld naar een nieuwe versie. Deze moet vooral gebruikersvriendelijker worden, zowel voor de ambtelijke organisatie als het gemeentebestuur.

2.3. Bestuur & organisatie

Informatieveiligheid is van de hele gemeentelijke organisatie. Vaak is in beleidsdocumenten vastgelegd dat het lijnmanagement hier verantwoordelijkheid voor draagt. Managers moeten erop toezien dat richtlijnen bij medewerkers bekend zijn en worden nageleefd. Vanuit wet- en regelgeving is een aantal functies verplicht gesteld. Zo verplicht de AVG gemeenten om een Functionaris Gegevensbescherming (FG) in dienst te hebben en dient de Chief Information Security Officer (CISO) volgens de BIO2 zo gepositioneerd te zijn binnen de organisatie dat hij onafhankelijk van de lijn kan adviseren over informatieveiligheid[2].

Het college is eindverantwoordelijk voor de informatieveiligheid van de organisatie. Het college stelt beleid vast en ziet erop toe dat onbevoegden zich geen toegang kunnen verschaffen tot gemeentelijke informatiesystemen. Mocht dit toch gebeuren, dan kan het nodig zijn om een crisisorganisatie in te richten.

De gemeenteraad is bevoegd de kaders te stellen en het college te controleren. Allereerst wordt van de gemeenteraad verwacht dat hij voldoende middelen beschikbaar stelt, zodat de gemeente aan wet- en regelgeving kan voldoen. In de praktijk blijkt vaak dat raden het lastig vinden om hun controlerende rol goed in te vullen omdat informatieveiligheid als een technisch onderwerp wordt beschouwd[3]. Maar net als bij andere beleidsterreinen is ook hier aan de gemeenteraad om kaders te stellen en te controleren of de gemeente recht- en doelmatig handelt.

2.4. Weerbaarheid

Elke gemeente neemt maatregelen om onbevoegd gebruik van data en informatiesystemen tegen te gaan. Het gaat hierbij niet alleen om het risico op een hack, maar ook onbedoeld verlies van geclassificeerde informatie, of een IT-leverancier van de gemeente die een fout maakt, waardoor de continuïteit van de gemeentelijke dienstverlening in gevaar komt.

---

[2] CISO (Chief Information Security Officer): Verantwoordelijk voor het ontwikkelen en implementeren van het informatiebeveiligingsbeleid binnen een organisatie. Houdt toezicht op de beveiliging van informatie en zorgt ervoor dat de organisatie voldoet aan relevante wet- en regelgeving. Heeft kennis van informatiebeveiliging, risicoanalyse en beveiligingstechnieken. De CISO kan in zijn taken worden bijgestaan door een Information Security Officer, een ISO.
FG (Functionaris Gegevensbescherming) of DPO (Data Protection Officer): Houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) binnen een organisatie. Adviseert en rapporteert aan het hoogste managementniveau over privacykwesties. Is verplicht voor overheidsinstanties en organisaties die op grote schaal bijzondere persoonsgegevens verwerken.
PO (Privacy Officer): Ontwikkelt en voert het privacybeleid uit binnen een organisatie. Ondersteunt de FG en fungeert als juridisch adviseur op het gebied van privacy. Is niet verplicht zoals de FG, maar speelt een belangrijke rol in het waarborgen van privacy binnen de organisatie.

[3] Toezicht in het kader van de Cyberbeveiligingswet – Naar gelaagd en geslaagd toezicht, Onderzoek van PBLQ in opdracht van de VNG, IPO en de Unie van Waterschappen, juli 2025

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Bij weerbaarheid gaat het in eerste instantie om preventieve maatregelen die worden genomen om digitale verstoringen te voorkomen. Voorbeelden van deze maatregelen zijn het autorisatiebeleid en de toegang van medewerkers tot de verschillende informatiesystemen. Ook bewustwordingsactiviteiten als (online) opleidingen en pentesten zijn belangrijke preventieve maatregelen om verstoringen te voorkomen. Bij opleidingen gaat het niet alleen over de vraag of er voldoende wordt aangeboden, maar ook over de mate waarin opleidingen (al dan niet verplicht) worden gevolgd en de wijze waarop hierop wordt gemonitord en gestuurd. Pentesten[4] kunnen zowel betrekking hebben op de technische beveiliging van informatiesystemen als op de medewerkers (human factor pentesten). Voorbeelden van deze laatste categorie zijn ‘phishing mails’ en mystery guests, die proberen om fysiek het gemeentehuis binnen te komen en toegang te krijgen tot informatiesystemen.

Weerbaarheid gaat daarnaast over de respons van de gemeente als een digitale verstoring zich voordoet. Reageert de gemeente adequaat? Wordt er tijdig opgeschaald en een crisisorganisatie ingericht en worden hier de juiste beslissingen genomen? Met oefeningen en simulaties van digitale verstoringen kan de gemeente inzicht krijgen in de effectiviteit van de respons op een digitale verstoring.

[4] Een pentest, oftewel penetratietest, is een gecontroleerde en gesimuleerde cyberaanval op een computersysteem, netwerk of webapplicatie met als doel om kwetsbaarheden te identificeren voordat kwaadwillenden dat doen.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

3. Proces en organisatie

In dit hoofdstuk gaan we in op deelvraag 1 en geven we een overzicht van wat de gemeente Stichtse Vecht doet op het gebied van informatieveiligheid. We kijken daarbij naar het beleid, risicomanagementprocedures en welke beheersmaatregelen er getroffen worden. Ook besteden we aandacht aan de omgang van de gemeente met datalekken.
Conclusies uit dit hoofdstuk:

- Stichtse Vecht beschikt over BIO-conform informatiebeveiligingsbeleid, maar het beleidsplan (met looptijd tot 2023) is verouderd;
- De gemeente Stichtse Vecht voldoet niet volledig (73%) aan de BIO;
- De 10 maatregelen van de Cyberbeveiligingswet zijn nog niet allemaal ingeregeld.
- De gemeente heeft maatregelen genomen om persoonsgegevens te beschermen. Ook is er een protocol datalekken waarin is vastgelegd dat belanghebbenden over een datalek worden geïnformeerd.

3.1. Strategisch informatiebeveiligingsbeleid

De gemeente Stichtse Vecht heeft een strategisch informatiebeveiligingsbeleid 2020-2023, dat is opgesteld door de CISO[5]. Dit beleid blijft van kracht totdat er meer duidelijkheid is over de invoering van de BIO2 en de Cyberbeveiligingswet[6]. De gemeente staat echter niet stil en is bezig met een grote transitie op het gebied van informatievoorziening (IV) en ICT. De afgelopen jaren heeft de gemeente gewerkt aan het ontwikkelen van de (ICT) organisatie, mede op basis van het coalitieakkoord 2022-2026 waarin de ambitie is opgenomen om het fundament op orde te krijgen[7].

Het beleid is opgesteld naar het model van de VNG. De tien bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de VNG vormen een belangrijk uitgangspunt voor het beleid, met name met betrekking tot de rol van het bestuur[8]: De basis voor het strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De gemeente voldoet op dit moment nog niet aan de BIO.

De gemeente Stichtse Vecht heeft de volgende strategische doelen opgesteld:

Strategische doelen
• 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.

De uitgangspunten van het beleid van de gemeente Stichtse Vecht zijn als volgt:

[5] Bron: *Strategisch Informatiebeveiligingsbeleid 2020-2023 versie 1.1,* (geactualiseerd in 2024).
[6] Dit is opgenomen in de Memo *Uitstellen actualisering Strategisch Informatiebeveiligingsbeleid*, (14 oktober 2024).
[7] Zie ook: *Coalitieakkoord 2022-2026 'Bouwen aan een stevig fundament voor Stichtse Vecht'*, p. 5-6.
[8] Bron: *De tien bestuurlijke principes voor informatiebeveiliging*, VNG, (2019). Geraadpleegd via: https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Uitgangspunten van het beleid

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang[9]. Het college van B&W is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de 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, organisatiebrede 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 kritieke 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.

Tactisch beleid

Het strategisch informatiebeveiligingsbeleid wordt uitgewerkt in tactische plannen en richtlijnen voor de verschillende onderdelen van het beleid. De CISO en ISO werken dit uit, waarna het tactisch beleid wordt vastgesteld door de directie. Team data en informatiemanagement (D&I) stelt beleid op met een sterke technische component, waarbij advies wordt ingewonnen bij de CISO. Het eigenaarschap van het technische beleid ligt echter bij D&I, de uitvoering van het beleid kan vervolgens wel in samenwerking met de CISO/ISO opgepakt worden. Het tactisch beleid dat door D&I moet worden opgesteld is ten tijde van dit onderzoek nog niet voor alle onderdelen uitgewerkt, hoewel het strategisch informatiebeveiligingsbeleid al sinds 2020 van kracht is. Uit de gesprekken komt naar voren dat dit te maken heeft met onvoldoende capaciteit binnen D&I, waardoor het opstellen van beleid blijft liggen. Dat betekent niet dat er in de uitvoering niks gebeurt, het formeel vastleggen op papier blijft echter nog achter.

Jaaropdrachten

De uitwerking van het tactisch beleid in concrete maatregelen vond tot en met 2023 plaats in de Jaaropdracht Gegevensbescherming en Informatieveiligheid. Sinds de inwerkingtreding van het strategisch beleid werd er jaarlijks een Jaaropdracht Gegevensbescherming en Informatieveiligheid

[9] Welke informatie hieronder valt wordt bepaald aan de hand van risicoanalyses, zo stelt het beleid. Aan de hand van de geïdentificeerde risico’s worden maatregelen getroffen om de informatie te beveiligen.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

uitgeschreven waarin de werkzaamheden voor dat jaar uiteengezet waren[10]. De organisatie is hier echter na 2023 mee gestopt. De FG, CISO en Privacy Officers zijn verantwoordelijk voor het uitvoeren en borgen van de opdrachten uit de jaaropdracht. Uit de interviews bleek dat de jaaropdrachten in de praktijk vooral op initiatief en met input van de CISO opgesteld en uitgevoerd werden. Het eigenaarschap voor de uitvoering van de jaaropdracht binnen de organisatie ontbrak. Door het stoppen met de jaaropdracht is echter ook een regulier plannings- en verantwoordingsinstrument verdwenen.

De onderwerpen die voor 2023 op de planning stonden hadden vooral te maken met privacy. Het ging daarbij om het uitvoeren van DPIA's[11], het actualiseren van het verwerkingsregister, het actualiseren van het privacybeleid, het actualiseren van de procedure "rechten van betrokkenen" en het protocol meldplicht datalekken, het vergroten van bewustwording omtrent gegevensbescherming. Op het gebied van informatieveiligheid waren er enkele actiepunten met betrekking tot het verhogen van digitale weerbaarheid, het implementeren van maatregelen in het kader van de BIO en het laten uitvoeren van de pentest. De pentest is in 2022 uitgevoerd. Een deel van de overige activiteiten stond ook in de jaaropdracht van 2022 al op de planning, maar is in dat jaar niet uitgevoerd. Het gaat daarbij om het uitvoeren van DPIA's, het actualiseren van het verwerkingsregister, het actualiseren van de procedure "rechten van betrokkenen" en het protocol meldplicht datalekken en het laten uitvoeren van een pentest. Een aantal acties, zoals het implementeren van maatregelen in het kader van de BIO, zijn doorlopende acties die dus in beide jaren op de planning stonden. Naar aanleiding van de ENSIA rapportage 2024 en de GAP analyse zijn in 2025 7 verschillende projecten opgepakt om de informatieveiligheid te verhogen. Uit de gesprekken blijkt dat er wel wordt gerapporteerd aan de gemeentesecretaris en het college, maar niet op basis van een reguliere verantwoordingsrapportage. Daardoor is er ook geen overzicht van risico's waarop gestuurd kan worden.

3.2. Rollen en verantwoordelijkheden

In het strategisch informatiebeveiligingsbeleid worden verschillende rollen gedefinieerd. Dit is op basis van het Three Lines of Defence model. De eerste lijn wordt gevormd door het management en is verantwoordelijk voor risicomanagement in de processen. De tweede lijn bestaat uit specialisten die de eerste lijn ondersteunen bij het uitvoeren van de activiteiten die nodig zijn voor risicomanagement. De derde lijn houdt toezicht op de werkzaamheden van de eerste en tweede lijn. In de gemeente Stichtse Vecht 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. In de praktijk voeren de CISO en de ISO vaak samen de tweede en derde lijn uit. Informatiebeveiliging is echter een verantwoordelijkheid van alle medewerkers van de gemeente. Iedereen moet zich bewust zijn van de risico's die er zijn en op zorgvuldige wijze omgaan met de gegevens en informatie waar hij of zij tijdens het werk mee te maken krijgt.

Het college van B&W is bestuurlijk eindverantwoordelijk voor informatiebeveiliging en risicomanagement binnen de gemeente en rapporteert daarover aan de gemeenteraad, die daarbij een kaderstellende en controlerende rol heeft. Binnen het college is er een portefeuillehouder aangesteld voor informatiebeveiliging. De gemeentesecretaris is ambtelijk eindverantwoordelijk voor informatiebeveiliging en rapporteert aan het college en de portefeuillehouder. Het directieteam van de gemeente is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op het strategisch beleid. De directie rapporteert hierover aan het college en de portefeuillehouder. De uitvoering van de informatiebeveiliging binnen de gemeentelijke processen is de verantwoordelijkheid van het

[10] Zie ook *Jaaropdracht Gegevensbescherming & Informatieveiligheid 2022* en *Jaaropdracht Gegevensbescherming & Informatieveiligheid 2023*.
[11] Een Data Protection Impact Assesment (DPIA) is een verplicht onderzoek onder de AVG dat organisaties moeten uitvoeren om de privacyrisico's van een (nieuwe) gegevensverwerking in kaart te brengen, voordat deze start.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

lijnmanagement (de teammanagers). Zij zijn eigenaren van informatiebronnen- en systemen die gebruikt worden door de gemeente. Het lijnmanagement legt verantwoording af aan het directieteam.

De Chief Information Security Officer (CISO) is verantwoordelijk voor de organisatie van informatiebeveiliging en heeft als taak om de informatieveiligheid van de gemeente op een hoger niveau te brengen en in de organisatie te borgen. De CISO rapporteert aan de gemeentesecretaris en de portefeuillehouder.

Op het gebied van privacy zijn de privacy officers verantwoordelijk voor de uitvoering van het privacybeleid en alle activiteiten die daarbij horen. Zij rapporteren hierover aan het directieteam. De Functionaris Gegevensbescherming (FG) ziet er als onafhankelijke toezichthouder op toe dat de gemeente persoonsgegevens beschermt en beveiligt volgens de normen van de AVG. De FG rapporteert hierover rechtstreeks aan het college.

3.3. Risicomanagement

Het strategisch informatiebeveiligingsbeleid schetst dat de aanpak die de gemeente hanteert voor informatiebeveiliging, gebaseerd is op risicobeheersing. Informatiebeveiliging wordt door de gemeente gezien als een continu verbeterproces met de PDCA-cyclus als uitgangspunt. In de jaarstukken van de gemeente worden risico's met betrekking tot informatiebeveiliging beschreven in de vaste paragraaf 'weerstandsvermogen en risicobeheersing'[12]. Onder de Cyberbeveiligingswet wordt risicomanagement een verplicht onderdeel waar veel aandacht aan besteed moet worden, om vervolgens de juiste maatregelen te kunnen treffen. Hier wordt in hoofdstuk 6 verder op ingegaan.

Uit de gesprekken blijkt dat risicomanagement binnen de gemeente Stichtse Vecht nog volop in ontwikkeling is. Er is een duidelijke wens om te groeien naar een meer planmatige aanpak en sturing op risico's via een ISMS. In het strategisch informatiebeveiligingsbeleid staat dat één van de verantwoordelijkheden van teammanagers het uitvoeren van quickscans is op basis van de BIO om risico-afwegingen te kunnen maken. Op basis van risico's worden vervolgens beveiligingsmaatregelen bepaald.[13] Uit het onderzoek is gebleken dat dit beleid niet structureel gevolgd wordt voor alle processen. De gemeente heeft 11 processen geïdentificeerd als kritiek en voor die processen zijn quickscans en Business Impact Analyses (BIA's) uitgevoerd.[14] Daarin worden de risico's binnen deze processen in kaart gebracht en worden bijbehorende maatregelen om deze risico's te mitigeren benoemd.

In 2024 is er een rekenkameronderzoek uitgevoerd naar risicomanagement in brede zin binnen de gemeente Stichtse Vecht. De hoofdconclusie uit dit onderzoek is dat de gemeente Stichtse Vecht de afgelopen jaren een stevig fundament heeft gebouwd op het gebied van risicomanagement. Toch is risicomanagement volgens de onderzoekers nog te weinig geborgd in de processen van de organisatie en is er sterke afhankelijkheid van de inzet van individuele medewerkers van de gemeente, waardoor een eenduidige werkwijze ontbreekt. Volgens de onderzoekers beschikt de gemeente over de benodigde capaciteit, kennis en instrumenten om het risicomanagement van de gemeente te verbeteren[15]. In het kader van de Cyberbeveiligingswet wordt het uitvoeren van risicoanalyses ten behoeve van informatiebeveiliging verplicht. In hoofdstuk 6 wordt hier nader op ingegaan. Het is voor de gemeente dus van groot belang om een gedegen risicomanagement procedure te hebben, die is geborgd in de organisatie en bij de juiste personen is belegd.

[12] Bron: Gemeente Stichtse Vecht *Jaarstukken 2022* en *Jaarstukken 2023.*
[13] Bron: Gemeente Stichtse Vecht (2024) *Strategisch Informatiebeveiligingsbeleid 2020-2023 versie 1.1,* p. 13.
[14] Bron: Diverse BIA's (2024).
[15] Bron: Rekenkamer Stichtse Vecht (2024) *Risicomanagement in de gemeente Stichtse Vecht*.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

3.4. Risico's en kwetsbaarheden

Begin 2025 is er een GAP-analyse uitgevoerd naar de BIO-compliance op basis van de resultaten van de ENSIA audit van 2024[16]. Deze analyse is eerder uitgevoerd in 2021 en 2023, waardoor inzichtelijk is wat de voortgang is. Er is geen uitgewerkt tactisch beleid waarin het proces voor het uitvoeren van deze GAP-analyses staat beschreven. De GAP-analyses worden incidenteel uitgevoerd maar dit is niet geborgd in de organisatie. Er ontbreekt een PDCA-cyclus voor dit proces.

In 2021 was de totaalscore op het voldoen aan de BIO van de gemeente 64%, in 2023 was dit 76% en in 2024 daalde de score weer tot 73%. Deze daling komt voort uit dalingen op de thema's toegangsbeveiliging, beveiliging bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties en naleving. Met name communicatiebeveiliging en naleving tonen grote dalingen van beide 25% ten opzicht van 2023[17]. Dat is een zorgelijke ontwikkeling.

Op basis van deze aandachtspunten is er een overzicht gemaakt van acties die moeten worden uitgevoerd om wel aan de BIO te kunnen voldoen. Op basis van een risicoanalyse is er een prioritering gemaakt van deze acties, inclusief een planning voor de uitvoering van de acties[18].

3.5. Datalekken

Naast de BIO moet de gemeente ook voldoen aan de AVG. Eén van de strategische doelen uit het strategisch informatiebeveiligingsbeleid is *Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.* Eén van de verplichtingen van de AVG is dat organisaties alle datalekken moeten documenteren, ook de datalekken die niet worden gemeld aan de Autoriteit Persoonsgegevens (AP). Stichtse Vecht registreert de datalekken, net als andere beveiligingsincidenten, in TOPdesk.

Voor het behandelen van (mogelijke) datalekken gebruikt de gemeente een protocol[19]. De laatste versie van dit protocol is in 2019 vastgesteld. Hierin staat nauwkeurig beschreven welke procedures er gevolgd moeten worden. De FG beoordeelt per datalek of de betrokkenen geïnformeerd moeten worden. De FG doet dat vanuit zijn of haar onafhankelijke rol. De privacy officer heeft daarbij een adviserende rol om te zorgen dat de melding voldoet aan de criteria van de AVG.

In 2024 zijn er 37 meldingen gedaan van mogelijke datalekken[20]. Na onderzoek bleek dat 30 van deze meldingen daadwerkelijk een datalek betroffen. Hier zijn vervolgens maatregelen voor getroffen en is er indien nodig melding gemaakt bij de AP en/of betrokkenen.

In zowel de Jaaropdracht Gegevensbescherming en Informatieveiligheid 2023 als de Jaaropdracht 2022 was het actualiseren van het protocol meldplicht datalekken één van de actiepunten. De actualisatie was met name nodig op het punt van de rollen bij de afwikkeling van datalekken in het algemeen en het informeren van betrokkenen in het bijzonder. Uit het onderzoek blijkt dat het er een nieuw concept protocol bestaat. Dit protocol is echter nog niet formeel vastgesteld.

[16] Bron: *GAP-analyse BIO 2024,* (2024).
[17] De daling kan ook een gevolg zijn van een kritischer invulling van de ENSIA vragenlijst en GAP analyse.
[18] Bron: *Prioritering maatregelen Infra en KA 0.3*, (2025).
[19] Bron: *Protocol meldplicht datalekken*, (2019).
[20] Bron: *Bijlage met nadere uitwerking geregistreerde datalekken periode januari t/m december 2024*, (2024).

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

4. Mens

In dit hoofdstuk beantwoorden wij de deelvragen die betrekking hebben op de bewustwording en competentieontwikkeling op het gebied van digitale veiligheid bij de medewerkers van de gemeente Stichtse Vecht. Om deze vragen te beantwoorden hebben wij, naast interviews en een documentstudie, een focusgroep uitgevoerd. Bij deze focusgroep waren 14 medewerkers van twee verschillende afdelingen aanwezig. Aan de hand van stellingen hebben wij met hen het gesprek gevoerd over hoe er op de werkvloer met informatiebeveiliging wordt omgegaan. Deze methode levert betrouwbaarder informatie op dan bijvoorbeeld een vragenlijst, waar vaak sociaal wenselijke antwoorden gegeven worden.
Conclusies uit dit hoofdstuk:

- De medewerkers van de gemeente Stichtse Vecht zijn bekend met het gemeentelijk beleid op het gebied van privacy en informatiebeveiliging. Het belang van dit beleid wordt onderkend en medewerkers volgen richtlijnen en instructies.
- Er worden trainingen aangeboden op het gebied van informatiebeveiliging. Ook is de tweefactor-authenticatie ingeregeld.

4.1. Leer- en ontwikkelprogramma's

Informatiebeveiliging is een vast onderdeel in het ontwikkelprogramma van de gemeente. Zowel in het onboardingprogramma voor nieuwe medewerkers als in het programma voor zittende medewerkers wordt hieraan aandacht besteed. Ook in de organisatiecultuur is aandacht voor informatieveiligheid. Zo is in de ambtseed, die nieuwe medewerkers afleggen, opgenomen dat medewerkers zorgvuldig moeten omgaan met informatiesystemen en gegevens. Daarnaast wordt ook in de trainingen op het gebied van integriteit aandacht besteed aan digitale veiligheid. Voorts wordt een open organisatiecultuur nagestreefd, waarbij medewerkers gestimuleerd worden om fouten, die bijvoorbeeld leiden tot een datalek, te melden. Dit komt onder andere tot uiting in de slogan: 'Je bent een held als je meldt' en verschillende activiteiten die jaarlijks in oktober, 'de maand van de veiligheid' worden georganiseerd.

In het inwerkprogramma voor nieuwe medewerkers zijn vijf online microlearnings en een bewustwordingssessie over digitale veiligheid opgenomen. Deze moeten de eerste drie maanden na indiensttreding verplicht worden gevolgd. De bewustwordingssessie wordt verzorgd door de CISO en de PO. Dat zorgt voor bekendheid van deze medewerkers en inhoudelijk maatwerk dat is toegespitst op de organisatie Stichtse Vecht.

Digitale veiligheid is ook verplichte kost voor zittende medewerkers. In een uitgebreide e-learning, die bestaat uit zeven modules over verschillende onderdelen van digitale veiligheid en privacy, wordt kennis en informatie overgedragen. Elke module wordt afgesloten met een test van 10 vragen waarvan er minstens 8 goed beantwoord moeten worden. Als dit programma met goed gevolg wordt afgesloten, volgen medewerkers jaarlijks een lichter programma dat bestaat uit twee verschillende modules met elk een test.

Naast deze structurele activiteiten worden ook incidentele activiteiten ingezet om het I-bewustzijn te vergroten. Voorbeelden hiervan zijn een summerschool, een escape room en extra werkconferentie voor de gemeenteraad die in de aanloop naar de Cyberbeveiligingswet is georganiseerd.

Leidinggevenden moeten sturen op deelname van hun medewerkers aan de (verplichte) programma's. Hierbij is nog verbetering mogelijk. Zo is in 2025 het sturen op verplichte deelname aan opleidingsprogramma's nog niet als KPI vastgesteld. Wel worden managers ondersteund bij het voeren van lastige gesprekken.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

4.2. Phishing tests en Mystery Guest

De CISO voert periodiek een phishing test uit om na te gaan hoe het I-bewustzijn zich in de organisatie ontwikkelt. Bij zo'n test wordt een 'fake mail' verzonden naar de medewerkers waarin gevraagd wordt om gevoelige informatie achter te laten (gebruikersnaam en wachtwoord). Uit een vergelijking tussen de verschillende testen blijkt dat het I-bewustzijn de afgelopen jaren is toegenomen. Toch hebben in de laatste test (van juni 2024) nog 90 van de 716 ontvangers van de phishing mail op de link geklikt. Van deze 90 medewerkers hebben er vier gegevens achtergelaten (tegen 33 bij de vorige test). Een belangrijke conclusie uit de laatste phishing test is dan ook dat er blijvende aandacht nodig is voor informatiebeveiliging.

In aanvulling op deze phishing test is in 2023 eenmalig een mystery-guest-onderzoek uitgevoerd. Hierbij probeert een onderzoeker (de mystery guest) zich onbevoegd toegang te verschaffen tot de beveiligde gedeelten van het gemeentehuis om vervolgens te kijken of hij bij (vertrouwelijke) informatie kan komen. Dit betreft zowel digitale informatie (via openstaande en onbemande computers) als fysieke informatie (documenten op bureaus en/of mappen in kasten die niet op slot zijn. De mystery guest wist eenvoudig binnen te komen en ook kon hij makkelijk bij (vertrouwelijke) gegevens. Op basis van deze test heeft de CISO onder andere aanbevelingen gedaan aan de directie gericht om het clean-desk- en clear-screen-beleid aan te passen. Uit de focusgroep blijkt dat medewerkers van deze aanpassingen op de hoogte zijn.

4.3. Uit de focusgroep: balans tussen veiligheid en gebruikersvriendelijkheid

Uit het gesprek met medewerkers in de focusgroep blijkt dat de (aanwezige) medewerkers zich bewust zijn van het belang van digitale veiligheid. Zij zijn op de hoogte van het beleid en weten over het algemeen wat te doen in geval van een datalek. Medewerkers geven aan dat een grote digitale verstoring, bijvoorbeeld door een hack, niet uit te sluiten valt. Zij vragen zich af of de gemeente zich hierop heeft voorbereid. Op de eigen afdeling is wisselend aandacht voor digitale veiligheid. Zeker als de werkdruk hoog is, gaat 'het werk' voor informatieveiligheid. Sommige medewerkers geven aan dat zij een actievere rol van hun leidinggevende verwachten op dit domein. Bijvoorbeeld door het onderwerp vaker op de agenda te zetten en te bespreken in bilaterale gesprekken.

Een rode draad door het gesprek is de spanning tussen gebruikersvriendelijkheid aan de ene kant en informatiebeveiliging aan de andere. Medewerkers geven aan dat zij in een open omgeving werken met burgers, bedrijven en (zorg)instellingen waarmee zij regelmatig via verschillende systemen informatie uitwisselen. Elk van die systemen is op een eigen manier beveiligd met wachtwoorden en inlogcodes. Medewerkers klagen over het aantal wachtwoorden en de frequentie van inloggen (voor sommige systemen elke 30 minuten). Het zorgt niet alleen voor vertraging, maar ook dat zij op zoek gaan naar snellere en alternatieve manieren van het delen en opslaan van gegevens en bestanden waarbij de informatieveiligheid niet is gegarandeerd . Een aantal medewerkers is van mening dat de balans tussen gebruikersvriendelijkheid en informatieveiligheid ernstig is verstoord.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

5. Techniek

In dit hoofdstuk wordt ingegaan op technische maatregelen van digitale veiligheid in de gemeente Stichtse Vecht. Centraal staat deelvraag drie: *Zijn gegevens bij de gemeente goed beschermd tegen de toegang door onbevoegden?* Deze vraag wordt beantwoordt aan de hand van een aantal onderwerpen: ICT-infrastructuur en cloud, inkoop en leveranciersmanagement, penetratietesten, logging[21], autorisaties, incidentmanagement en risico's en kwetsbaarheden.

Het is aan de gemeente om een risico-afweging te maken en daar (technische) maatregelen aan te koppelen. In dit rapport voor de gemeenteraad zoomen we in op of de voorgenomen technische maatregelen inderdaad zijn genomen en of processen worden gevolgd zoals beschreven in plannen en beleid.
Conclusies uit dit hoofdstuk:

- De gemeente heeft maatregelen genomen om de informatieveiligheid te borgen. Zo is het toegangsbeleid bekend bij alle medewerkers en wordt dat goed nageleefd.
- In het deltaplan ICT van de gemeente wordt impliciet rekening gehouden met Informatiebeveiliging, maar risicosturing is nog onvoldoende;
- De gemeente heeft een Cloudstrategie waarbij de applicaties worden overgebracht naar de Cloud. Hierdoor worden leveranciers verantwoordelijk voor de technische aspecten van informatiebeveiliging.
- Informatiebeveiliging wordt hierdoor een zaak van goed contractmanagement. De gemeente controleert bij de leveranciers van ICT Infra en kantoorautomatisering van team D&Q of zij de gemaakte afspraken op het gebied van informatiebeveiliging nakomen.

5.1. Deltaplan ICT en IV

De gemeente had tot 2023 nog eigen servers die sterk verouderd waren. Daarnaast werkten de systemen nog op Windows 2012 en Microsoft ging stoppen met de ondersteuning daarvan. Dit was aanleiding voor de gemeente om met grote spoed de infrastructuur over te brengen naar een serverpark bij Centric en de serverruimte bij de gemeente uit te zetten. De situatie was ontstaan door een combinatie van factoren. Zo was er onvoldoende geïnvesteerd in ICT en IV, waren verkeerde keuzes gemaakt en werd met de verkeerde strategische partner samengewerkt.

De gemeente werkt inmiddels aan een grote inhaalslag op het gebied van ICT en IV en heeft in 2024 het *Deltaplan ICT en IV* opgesteld[22]. Hiermee wordt een modernisering van de ICT en IV vormgegeven. Het Deltaplan ICT en IV is een overkoepelend document waarin een overzicht wordt gegeven van alle bestaande en nog op te stellen visies en beleidsstukken met betrekking tot de hele ICT en IV. Informatiebeveiliging is hier een onderdeel van. Het Deltaplan verbindt de verschillende uitdagingen op het gebied van ICT en IV met elkaar en is specifiek gericht op ontwikkeling van het professionaliseren van ICT en informatievoorziening. Het Deltaplan bestaat uit onder andere de volgende onderdelen:

1. Een visie op ICT infrastructuur (verwijzing naar reeds uitgevoerde datacentermigratie, Citrix/Windows upgrade) en kantoorautomatisering
2. Een geformuleerde Cloudvisie en rationalisering van het applicatielandschap[23]
3. Een visie op ICT, IV en beveiliging

[21] Logging is het systematisch vastleggen van gebeurtenissen, acties en processen binnen een IT-systeem, applicatie of netwerk. Het doel is om inzicht te krijgen in wat er gebeurt, wanneer het gebeurt, en door wie of wat het wordt veroorzaakt.
[22] Bron: *Deltaplan ICT en IVT*, (2024).
[23] De gemeente Stichtse Vecht hanteert de Cloud-tenzij visie voor het sourcen van IT-diensten en -oplossingen. Dit betekent dat het gebruik van clouddiensten en -oplossingen het uitgangspunt is, tenzij er specifieke redenen zijn om dit niet te doen (met name op het gebied van informatiebeveiliging, privacy, en kosten). Vanuit deze doelstelling wordt er naar gestreefd dat medio 2026 alle applicaties zijn ondergebracht zijn in een SAAS dienstverlening. De reden hiervoor is om zoveel mogelijk kostenreductie op de ICT-infrastructuur te realiseren. (bron Gemeente Stichtse Vecht (2024). *Deltaplan ICT en IV*, p.12-13)

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

1. **Visie ICT infrastructuur en kantoorautomatisering**

De uitgangspunten voor de ICT-infrastructuur zijn in december 2023 vastgesteld door de directie en op basis daarvan is de ICT-infrastructuur Europees aanbesteed..[24] De gemeente heeft inmiddels een leverancier geselecteerd en gaat eind 2025 over naar de nieuwe infrastructuur.[25]

De geformuleerde visie op ICT-infrastructuur en kantoorautomatisering is als volgt:

Visie ICT infrastructuur en kantoorautomatisering
Wij dragen zorg voor eigentijdse, betrouwbare en veilige informatie- en communicatietechnologie (ICT). Hiervoor is een goede ICT infrastructuur de basis waarbij de gemeente Stichtse Vecht de ambitie heeft om aan te sluiten bij de landelijke ontwikkelingen. De gemeente heeft niet de behoefte om zelf voorop te lopen maar kijkt vooral wat haalbaar is waarbij het zich richt op moderne en bewezen technologie. Het ICT landschap van de gemeente Stichtse Vecht bestaat uit de infrastructuur, de digitale werkplek en de applicaties waarmee gewerkt wordt.

2. **Visie Cloud**

De gemeente Stichtse Vecht heeft ook een visie geformuleerd op de ontwikkeling rond Cloud en SaaS-oplossingen[26]:

Visie Cloud
De gemeente Stichtse Vecht hanteert de Cloud-tenzij visie voor het sourcen van IT-diensten en -oplossingen. Dit betekent dat het gebruik van cloud diensten en -oplossingen het uitgangspunt is, tenzij er specifieke redenen zijn om dit niet te doen (met name op het gebied van informatiebeveiliging, privacy, en kosten).

In het Deltaplan ICT en IV is ook de rationalisering voor de visie opgenomen:

- Minder investeren in eigen datacenter, en minimaliseren eigen beheerlast. Voorkomen dure en complexe IT-infrastructuur migraties;
- Minder risicovolle en minder complexe aanbestedingen (voor business toepassingen);
- Kortere implementatietrajecten voor nieuwe diensten en oplossingen;
- Verbeteren flexibiliteit en schaalbaarheid van oplossingen en verhogen continuïteit ervan;
- Transparantie en voorspelbaarheid kosten. Afrekenen op basis van gebruik (pay-per-use);
- Sneller inspelen op veranderingen in de bedrijfsvoering;
- Makkelijker en sneller kunnen inzetten van marktinnovaties.

De gemeente streeft ernaar om medio 2026 alle applicaties onder te brengen in een SaaS-dienstverlening. Als reden wordt genoemd dat dit zoveel mogelijk kostenreductie op de ICT-infrastructuur gaat realiseren.[27]

De visie rond ICT infrastructuur en cloud laten zien dat de gemeente inzet op enerzijds modernisering van de techniek en anderzijds het meer uitbesteden van het technisch beheer van de ICT. De gemeente zet in betrouwbare, veilige en moderne ICT en wil aansluiten bij landelijke ontwikkelingen maar is daarin pragmatisch en wil niet vooroplopen.

3. **Visie ICT en IV beveiliging**

[24] Gemeente Stichtse Vecht (2024). *Deltaplan ICT en IV.*
[25] Gemeente Stichtse Vecht (2024). *Deltaplan ICT en IV*, p.10
[26] Een SaaS-oplossing is software die via internet wordt geleverd in plaats van dat de gebruiker deze zelf installeert. De software draait op de servers van de provider, die ook zorgt voor onderhoud, updates en infrastructuurbeheer. Gebruikers hebben toegang via een abonnement, meestal met een webbrowser, en hoeven zich geen zorgen te maken over de technische details.
[27] Gemeente Stichtse Vecht (2024). *Deltaplan ICT en IV,* p.13.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

De visie op ICT en IV beveiliging van de gemeente luidt als volgt:

Visie ICT en IV beveiliging
Wij zorgen ervoor dat de bescherming van waardevolle informatie onze core business is. Daarbij nemen wij naarmate de informatie waardevoller is des te meer maatregelen.

Kernprincipes voor de gemeente als het gaat om informatiebeveiliging en gegevensbescherming zijn toegankelijkheid en betrouwbaarheid van overheidsinformatie. Om gegevens te beschermen moeten er risicogebaseerde maatregelen getroffen worden. De gemeente houdt daarbij rekening met de BIO, NIS2, AVG, Archiefwet, Wet open overheid (Woo) en Wet politiegegevens (Wpg). De beveiliging van door de gemeente gebruikte systemen moet ook minimaal voldoen aan deze normen.

Het Deltaplan bevat een planning waarin op kwartaalniveau is aangegeven aan welk onderwerp wordt gewerkt tot en met 2026[28]. Voor informatieveiligheid staan er geen concrete doelen of mijlpalen in het plan. Het wordt uit het Deltaplan niet duidelijk welke activiteiten in het kader van informatieveiligheid worden ontplooid om aan de visie te werken. Er wordt niet gerapporteerd op kwartaalniveau.

5.2. Inkoop en leveranciersmanagement

De inzet van de gemeente op het uitbesteden van ICT en IV zorgt ervoor dat het eigen (technische) beheer minder belangrijk wordt, maar dat steeds meer zal worden ingekocht en afgenomen bij externe leveranciers. De gemeente kan zelf minder (technische) maatregelen treffen, maar moet daarover afspraken maken met leveranciers. Daarmee wordt ook de inkoop en het leveranciersmanagement steeds belangrijker voor de organisatie.[29]

De gemeente Stichtse Vecht heeft algemene inkoopvoorwaarden die gebaseerd zijn op het VNG model. Bij enkelvoudig onderhandse aanbestedingen heeft de gemeente een proces waarbij de Privacy officer en CISO meekijken (als ze worden aangehaakt) op de af te sluiten Verwerkersovereenkomst[30]. Daarnaast worden de GIBIT[31] inkoopvoorwaarden meegestuurd bij ICT-aanbestedingen, zo schetst het proces. In de GIBIT worden ook voorwaarden gesteld in het kader van informatiebeveiliging. De gemeente Stichtse Vecht heeft een standaard set aan eisen vanuit informatiebeveiliging en privacy[32] die worden opgenomen in een Programma van Eisen[33] bij een aanbesteding of inkooptraject.

Uit het documentonderzoek is gebleken dat de gemeente in 2024 bij de vijf leveranciers van ICT Infra en kantoorautomatisering van D&I door middel van een vragenlijst controleert of zij aan de informatiebeveiligingseisen voldoen. Over de uitkomsten van dit onderzoek heeft de CISO gerapporteerd aan het directieteam[34]. Uit de rapportage en de interviews blijkt dat de gemeente niet al haar leveranciers periodiek controleert op de eisen die worden gesteld.

[28] Er wordt niet over de voortgang bij deze planning gerapporteerd. Ook risico's bij de voortgang zijn niet inzichtelijk.
[29] Deze accentverschuiving is overigens niet expliciet opgenomen in het *Deltaplan ICT en IV.*
[30] Een verwerkersovereenkomst is een schriftelijke overeenkomst tussen een organisatie (de verwerkingsverantwoordelijke) en een externe partij (de verwerker) die namens die organisatie persoonsgegevens verwerkt. Deze overeenkomst is verplicht volgens de Algemene Verordening Gegevensbescherming (AVG) wanneer je persoonsgegevens laat verwerken door een derde partij, zoals een IT-dienstverlener.
[31] GIBIT staat voor Gemeentelijke Inkoop bij IT Toolbox. Het is een set van uniforme inkoopvoorwaarden die door de Vereniging van Nederlandse Gemeenten is ontwikkeld om gemeenten te ondersteunen bij het professioneel inkopen van ICT-diensten en -producten.
[32] Gemeente Stichtse Vecht (onbekend). *Basis PVE Aanbesteding* (status document onbekend).
[33] Er is niet onderzocht in hoeverre deze set eisen ook daadwerkelijk is opgenomen in contracten.
[34] Gemeente Stichtse Vecht (2024). *Rapportage Compliance & leveranciersmanagement*

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

5.3. Penetratietesten

Volgens het strategisch informatiebeveiligingsbeleid laat de gemeente, om kwetsbaarheden op te sporen en de digitale weerbaarheid te vergroten, jaarlijks een penetratietest (pentest) uitvoeren. In de praktijk is dit niet gebeurd. Eind 2022 is de meest recente pentest door de gemeente uitgevoerd.

Uit de documentanalyse blijkt dat er bij deze test enkele kritieke en hoog-risico-bevindingen waren. Het was mogelijk om significante verstoringen te veroorzaken en zeer gevoelige informatie te bemachtigen. Daarnaast was het o.a. mogelijk om volledige toegang tot het netwerk en systemen te verkrijgen. Naar aanleiding van de penetratietest is de gemeente gestart met het oplossen van de kritieke bevindingen of zijn de bevindingen (deels) opgelost. Uit de documentanalyse is niet gebleken of alle bevindingen uiteindelijk zijn opgevolgd.

5.4. Logging

Logging speelt een cruciale rol binnen informatiebeveiliging, omdat het helpt om inzicht te krijgen in wat er gebeurt binnen systemen, applicaties en netwerken. Door het vastleggen, *loggen,* van gebeurtenissen, zoals inlogpogingen, wijzigingen aan systemen of ongebruikelijke activiteiten, worden incidenten sneller gedetecteerd en kan er adequaat worden gereageerd. Dit draagt bij aan het vergroten van de digitale weerbaarheid van de organisatie: logging maakt het mogelijk om verdachte handelingen te traceren, patronen van misbruik te herkennen en bij een beveiligingsincident de oorzaak te achterhalen. Bovendien zijn loggegevens van groot belang bij het uitvoeren van audits en het voldoen aan wettelijke en normatieve eisen rondom informatieveiligheid. Zonder goede logging kunnen belangrijke signalen over kwetsbaarheden, misbruik of fouten over het hoofd worden gezien, waardoor de risico's voor de gemeente toenemen.

De gemeente heeft in concept een beleid voor logging en monitoring opgesteld[35] op basis van een handreiking van de IBD. Het beleid is nog niet vastgesteld. Met het beleid wordt bedoeld een kader te bieden voor logging en monitoring. In het conceptbeleid wordt geschetst dat logging en monitoring binnen de gemeente Stichtse Vecht wordt toegepast op de IT-infrastructuur, onderliggende applicaties en bijbehorende informatie. Het beleid maakt onderscheid tussen het loggen en monitoren op de volgende niveaus: netwerk, applicatie, beschikbaarheidscomponenten en gebruiksapparatuur.

Het beleid legt de verantwoordelijkheden van verschillende rollen vast. Zo moet de directie het beleid vaststellen en toezicht houden op naleving door het management. Het management is verantwoordelijk voor het beschikbaar stellen van middelen voor logging. De CISO adviseert en stelt kaders, zoals het beleid en ziet toe op de controle van het beleid.

Het technische beheer zorgt voor actieve logging op de belangrijkste[36] onderdelen. De logging moet beschikbaar zijn voor analyse of directe monitoring. Het technisch beheer richt zich op logging van veiligheid van de infrastructuur en gebeurtenissen van de bedrijfsprocessen. Voor SaaS-applicatie ligt het bij de leverancier. De interne beheerder coördineert en communiceert met de leverancier. De functioneel beheerder gaat over de functionele inrichting van de logging van bedrijfsprocessen.

In het beleid zijn daarnaast algemene uitgangspunten opgenomen. Deze zijn echter niet toegespitst naar de (uitgangs)situatie van Stichtse Vecht. Uit de documentanalyse blijkt daarnaast dat er diverse logging plaatsvindt bij verschillende leveranciers. Er vindt nog geen controle plaats op de logging en monitoring van leveranciers van SaaS-applicaties.

[35] Gemeente Stichtse Vecht (2025). *Logging en monitoring beleid.*
[36] In het beleid is niet gespecificeerd welke onderdelen dit zijn.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

5.5. Autorisaties

De gemeente heeft een beleid voor logische toegangsbeveiliging. Het beleid heeft als doel om invulling te geven aan het voorkomen van ongeautoriseerde toegang en het beheersen van de toegang tot informatiesystemen.[37] Het beleid van de gemeente heeft een aantal uitgangspunten, namelijk:

- De proceseigenaar[38] is verantwoordelijk voor wie geautoriseerd wordt en op welke manier dat gebeurt.
- Er worden in de regel geen 'algemene' (ongepersonaliseerde) identiteiten, zoals groepsaccounts, gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd.
- De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging of heeft een eigen voorziening voor gebruikersbeheer. Voor inwoners en bedrijfsleven gelden DigiD en eHerkenning.

In het beleid worden daarnaast de verantwoordelijkheden beschreven van de directie, proceseigenaar en CISO:

De directie is eindverantwoordelijk voor de juiste uitvoering van het logische toegangsbeveiligingsbeleid en geeft goedkeuring geeft op dit beleidsstuk. De proceseigenaar is direct verantwoordelijk voor de juiste en tijdige uitvoering van de taak door een gemachtigde gebruiker (bijv. functioneel beheerder) of is degene die de activiteit (bijv. controle) zelf uitvoert. Hiervoor wordt verantwoording afgelegd aan de directie. De Chief Information Security Officer (CISO) wordt vooraf geraadpleegd, adviseert en/of levert input bij een activiteit in het proces.[39]

Het beleid schetst daarnaast op algemene wijze welke mogelijkheden er zijn voor autorisatie en authenticatie binnen de gemeente. Zo wordt er gebruik gemaakt van Single-Sign-On waar mogelijk en Multifactor authenticatie (MFA) geldt altijd als toegang wordt verleend naar een 'vertrouwde zone'.[40]

Uit de gesprekken blijkt dat er autorisatiematrixen[41] aanwezig zijn binnen de gemeente. Bij sommige applicaties is de mogelijkheid beperkt om autorisaties toe te kennen. Ook geven medewerkers aan dat er om sommige autorisaties heen gewerkt kan worden. Zo kan de toegang tot de Bibob-omgeving[42] niet helemaal worden afgeschermd, blijkt uit het gesprek in de focusgroep. Het belang van autorisatie wordt onderstreept door het feit dat de accountant in de controle van de jaarrekening aandacht heeft voor dit onderwerp, zo geeft men ook in dit gesprek aan.

De proceseigenaren, veelal de managers, zijn verantwoordelijk voor de autorisaties, het beeld uit de gesprekken is dat de managers eigenlijk te weinig weten van de applicaties om de autorisaties goed te kunnen controleren.

[37] Gemeente Stichtse Vecht (2023). *Logische toegangsbeveiligingsbeleid.*
[38] In het Bedrijfscontinuïteitsplan van de gemeente zijn voor de negen kritieke bedrijfsprocessen proceseigenaren geïdentificeerd. Gemeente Stichtse Vecht (2024). *Bedrijfscontinuïteitsplan,* p. 6.
[39] Gemeente Stichtse Vecht (2023). *Logische toegangsbeveiligingsbeleid,* p. 10.
[40] Een vertrouwde omgeving betreft omgeving die door de gemeente Stichtse Vecht wordt beheerd.
[41] Een autorisatiematrix is een schema dat inzichtelijk maakt welke personen of rollen binnen een organisatie toegang hebben tot specifieke applicaties, systemen of gegevens. In dit schema wordt vastgelegd wie welke rechten heeft, bijvoorbeeld lezen, schrijven, wijzigen of verwijderen van informatie.
[42] De Wet Bibob staat voor Wet bevordering integriteitsbeoordelingen door het openbaar bestuur. Deze Nederlandse wet geeft overheidsinstanties zoals gemeenten de mogelijkheid om de achtergrond van bedrijven en personen te screenen voordat zij bijvoorbeeld een vergunning, subsidie of overheidsopdracht verstrekken. De Bibob omgeving is waar de gemeente informatie verwerkt in het kader van de uitvoering van die wet.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

5.6. Incidentmanagement

De gemeente heeft een incidentmanagementproces,[43] in concept opgesteld voor ICT incidenten in brede zin. Het proces is nog niet vastgesteld. De gemeente heeft nog geen apart proces voor beveiligingsincidenten. Uit de documentanalyse blijkt dat het beschreven proces niet (geheel) overeenkomst met het werkelijk gelopen proces. Ook blijkt dat er niet periodiek gerapporteerd wordt over ICT-incidenten, waardoor de PCDA cyclus op dit domein ontbreekt.

Over 2023 is een rapportage[44] beschikbaar met beveiligingsincidenten en datalekken. Deze rapportage geeft ook inzicht in de voorgaande jaren tot en met 2018. Het aantal datalekken is redelijk stabiel sinds 2019. Het aantal beveiligingsincidenten schommelt gedurende de jaren. In 2023 zijn er in vergelijking tot 2022 o.a. meer verloren toegangspassen gemeld. Er is geadviseerd nader te onderzoeken hoe dit terug te dringen. Uit de interviews blijkt dat op basis van dit onderzoek de toegangspassen nu herkenbaar zijn als zijnde van de Stichtse Vecht. We hebben niet kunnen vaststellen of dit heeft geleid tot minder verloren toegangspassen. Over 2024 is enkel een overzicht met datalekken bekend. Uit het onderzoek blijkt dat er een rapportage met datalekken en beveiligingsincidenten[45] is, maar dat deze niet is vastgesteld.

Uit de gesprekken blijkt dat de gemeente een SIEMSOC[46] functionaliteit deels heeft ingeregeld. Na volledige onboarding van de nieuwe beheerpartner wordt deze volledig ingericht. Op basis van welke randvoorwaarden deze functionaliteit werkt, is niet bekend.

[43] Gemeente Stichtse Vecht (2023). *Procesdocumentatie: ICT Incident Management* (Concept).
[44] Gemeente Stichtse Vecht (2024). *Memo Jaaroverzicht beveiligingsincidenten en datalekken 2023* (aan directie).
[45] Wij hebben deze rapportage niet gezien.
[46] Security Information and Event Management (SIEM) en Security Operations Center (SOC). Een SIEM-systeem verzamelt, analyseert en rapporteert over beveiligingsgerelateerde data uit verschillende bronnen binnen een organisatie, zoals netwerkapparatuur, servers en applicaties. Het SOC is een operationeel team dat verantwoordelijk is voor het bewaken, detecteren en afhandelen van beveiligingsincidenten. Door SIEM en SOC te combineren ontstaat een centrale plek waar monitoring, analyse en reactie op cyberdreigingen efficiënt en gecoördineerd worden uitgevoerd. SIEMSOC speelt een cruciale rol bij het waarborgen van informatieveiligheid en het minimaliseren van risico's binnen moderne organisaties.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

6. Cyberbeveiligingswet

In dit hoofdstuk gaan we nader in op hoe de gemeente Stichtse Vecht zich voorbereidt op de Cyberbeveiligingswet. De verplichtingen van de eisen van de Cyberbeveiligingswet zijn te vinden in bijlage C. Zorgplicht

De Cyberbeveiligingswet schrijft een aantal verplichte maatregelen voor die onder de zorgplicht vallen. Deze maatregelen komen grotendeels overeen met de huidige BIO. Tot nu toe is de BIO een (verplichte) zelfevaluatie, maar met de komst van de Cbw wordt deze ook wettelijk verplicht. De BIO wordt bovendien doorontwikkeld naar de BIO2, waarin de nadruk komt te liggen op het managementsysteem voor informatiebeveiliging. De VNG en de IBD adviseren om, vooruitlopend op de Cbw en de BIO2, werk te maken van de implementatie van de huidige BIO.

Belangrijkste conclusies uit dit hoofdstuk zijn:

- De gemeente Stichtse Vecht voldoet op dit moment voor 73% aan de BIO-norm. De organisatie heeft de afgelopen jaren stappen gezet richting een meer volwassen informatiebeveiliging, maar er zijn nog uitdagingen.
- De organisatie bereidt zich voor op de komst van de Cyberbeveiligingswet en de BIO2, ondanks beperkte capaciteit die hiervoor beschikbaar is. De prioriteiten van de gemeente voor de komende tijd zijn[47]:
    - Verbeteracties voor D&I uit de GAP-analyse doorvoeren
    - OT-processen (operationele technologie) verder in beeld brengen, inclusief eigenaarschap
    - BCM (business continuity management) verder inrichten en oefenen
    - Sturing op risicomanagement versterken
    - ISMS (information security management system) verder inrichten
    - Digitale weerbaarheid vergroten
- De gemeente beschikt sinds 2024 over een business continuity plan.
- Het college van B&W stuurt niet aantoonbaar op cyberbeveiligingsrisico's

Het is niet inzichtelijk hoe de gemeente de monitoring op deze acties heeft ingericht.

In de *Verkenning Digitale weerbaarheid* stelt de gemeente stelt dat er geen effectieve verbetercyclus voor informatiebeveiliging is. Verbeteracties worden ad-hoc uitgevoerd en de structuur ontbreekt om effectief de risico's, afspraken en voortgang te monitoren.[48]
De gemeente stelt dat dit leidt tot het niet nemen van juiste beheersmaatregelen om risico's te beheersen op gebied van informatiebeveiliging met imagoschade voor de gemeente als gevolg. Ook kan het bestuur niet de bestuurlijke verantwoordelijkheid nemen waardoor het bestuur aansprakelijk kan worden gesteld wanneer inbreuk wordt gemaakt op de '*zorgplicht'* vanuit de cyberbeveiligingswet.[49]

In de *Verkenning digitale weerbaarheid* schetst Stichtse Vecht dat er gebruik gemaakt wordt van automatisering voor besturing van industriële toepassingen, zoals de besturing van bruggen en sluizen, verkeerslichten, maar ook gebouwbeheerssystemen. Deze operationele technologie (OT) is wel onderdeel van de scope van de Cbw, maar momenteel valt dit vakgebied buiten de huidige werkzaamheden van de CISO.[50] De gemeente heeft nu onvoldoende inzicht in de beveiliging van de OT. Een onveilige OT-omgeving heeft directe impact op de veiligheid van burgers. De impact

[47] Bron: Prioritering maatregelen Infra en KA 0.3 (risico + capaciteit ingevuld)
[48] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.1.
[49] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.2.
[50] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.2.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

voor de gemeente zit in menselijk leed bij een desastreus incident en bijbehorende imagoschade/sancties, zo schetst de gemeente.

6.1. Registratie- en meldplicht en toezicht

De gemeente Stichtse Vecht heeft zich nog niet geregistreerd in het kader van de Cbw, op advies van de IBD. Wel heeft de gemeente toegang tot e-Herkenning waarmee de gemeente is voorbereid op registratie.

Het is voor de meldplicht onder andere van belang dat Stichtse Vecht een incidentresponsprocedure heeft. De gemeente heeft nu een incidentmanagementprocedure[51], deze procedure is echter niet vastgesteld. Hierbij moet rekening gehouden worden dat incidenten ook in het weekend binnen 24 uur gemeld moeten worden. Hiervoor werkt de gemeente al met een piketdienst; contactpersonen zijn altijd bereikbaar voor de IBD en/of de toekomstige toezichthouder.

Voor de overheid wordt de *Rijksinspectie Digitale Infrastructuur (RDI*) aangewezen als toezichthouder. Hoe het toezicht precies ingevuld gaat worden is nog niet bekend. Er zijn daardoor nog geen concrete vereisten om hierop voor te bereiden.

In de *Verkenning digitale weerbaarheid* schetst de gemeente dat uit de GAP-analyse[52] blijkt dat nog niet aan de huidige gestelde beheersmaatregelen uit de BIO wordt voldaan[53]. Daarbovenop vraagt de Cbw om extra beheersmaatregelen. Het risico van het niet voldoen aan het normenkader omschrijft de gemeente als een toename van beveiligingsincidenten, in de vorm van technische kwetsbaarheden tot het niet kunnen uitvoeren van gemeentelijke taken en niet in control zijn. In het kader van de Cbw kan hierdoor versterkt toezicht worden ingezet met uiteindelijke financiële sancties als gevolg.[54]

6.2. Bedrijfscontinuïteit

Onder de Cyberbeveiligingswet is het verplicht om maatregelen te treffen ten behoeve van bedrijfscontinuïteit. De gemeente Stichtse Vecht heeft in 2024 bedrijfscontinuïteitsbeleid en een bedrijfscontinuïteitsplan opgesteld[55]. Deze documenten moeten nog worden vastgesteld. Het bedrijfscontinuïteitsbeleid is van toepassing op de kritieke bedrijfsprocessen van de gemeente, waarbij een verstoring grote impact heeft op de bedrijfsvoering. Het bedrijfscontinuïteitsplan is voornamelijk gericht op cyberincidenten. In dit plan is uitgewerkt hoe de crisisorganisatie van de gemeente ingericht is, welke rollen en verantwoordelijkheden er zijn en welke activiteiten ondernomen moeten worden. Daarbij wordt onderscheid gemaakt tussen de koude en de warme fase. De warme fase is de fase waarin er een crisis is. In dit fase treedt het bedrijfscontinuïteitsplan in werking. De gemeentesecretaris is dan het hoofd van de bedrijfscontinuïteitsorganisatie, waarin onder andere ook de CISO, de manager D&I en de Privacy Officer zitting hebben. Als er geen sprake van een crisis ligt de focus op het treffen van preventieve maatregelen en voorbereidingen op een mogelijke crisis. Een van deze voorbereidingen is een crisisoefening. Deze is in Stichtse Vecht nog nooit uitgevoerd. Wel staat een oefening in de planning in de aanloop naar de Cyberbeveiligingswet. Ook is eerder dit jaar (op 5 maart 2025) deelgenomen aan de Cyberoefendriehoek in Amersfoort.

[51] Zie paragraaf 5.6.
[52] Uitgevoerd oktober 2023.
[53] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.3.
[54] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.3.
[55] Bron: *Bedrijfscontinuïteitsbeleid gemeente Stichtse Vecht v1.0*, (2024) en *Bedrijfscontinuïteitsplan (BCP) GSV v1.0*, (2024).

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Team Openbare Orde en Veiligheid (OOV) heeft bovendien een aantal documenten opgesteld met betrekking tot crisisbeheersing die ook voor een interne crisis als leidraad kunnen dienen. Zo is er een handboek voor wanneer er tijdens een crisis noodopvang of voorziening in primaire levensbehoeften nodig is voor inwoners[56]. Ook zijn er handboeken voor de nazorg[57] en de inzet van ondersteunend personeel aan de crisisorganisatie[58]. De gemeente Stichtse Vecht is ook betrokken bij het regionaal crisisplan voor de veiligheidsregio Utrecht[59].

In de koude fase[60] is het college van B&W verantwoordelijk voor het bewaken van de bedrijfscontinuïteit en het beschikbaar stellen van de benodigde middelen aan de organisatie om dit te borgen. In de Cyberbeveiligingswet is opgenomen dat bestuurders verplicht een opleiding moeten volgen in risicomanagement. Daarmee wordt de rol van bestuurders tijdens de koude fase uitgebreid, aangezien zij in staat moeten zijn om informatiebeveiligingsrisico's te duiden en te beoordelen welke mitigerende maatregelen getroffen moeten worden.

Specifiek voor de continuïteit van de ICT-dienstverlening die nodig is voor het uitvoeren van bedrijfskritieke processen wordt er momenteel door de gemeente gewerkt aan een kritieke-verstoringen-proces, als aanvulling op het incidentmanagementproces[61]. Dit proces is nog niet vastgesteld. Ook zijn er voor alle elf kritieke bedrijfsprocessen business impact analyses (BIA's) uitgevoerd. Met een BIA wordt in kaart gebracht welke impact een verstoring in deze processen heeft.

In de *Verkenning digitale weerbaarheid* schetst de gemeente dat een bedrijfscontinuïteitsproject is afgerond in 2024, maar dat daar zijn nog verbeterpunten uit gekomen. Die opvolgen is belangrijk om de gemeentelijke bedrijfscontinuïteit te borgen, zodat de gemeente in geval van een incident de kritieke processen binnen maximaal een dag weer kan hervatten.[62]
Bij onvoldoende borging van de gemeentelijke bedrijfscontinuïteit kunnen bij incidenten gemeentelijke taken mogelijk niet worden uitgevoerd.[63]

6.3. De rol van het bestuur

Zoals eerder is gemeld zijn de BIO- en ENSIA-rapportage aanknopingspunten voor sturing door het college van B&W en de gemeenteraad. Uit de focusgroep met de raad en het interview met de portefeuillehouder in het college bleek echter dat men niet bekend was met de BIO. En men wist dus ook niet of de gemeente voldeed aan de baseline.

Compliance met de BIO is een goede voorbereiding op de Cyberbeveiligingswet. Hiervoor is meer bestuurlijke en ambtelijke aandacht nodig. Zeker gezien het bestuur onder de Cyberbeveiligingswet meer verantwoordelijkheid krijgt. Zo schrijft de wet voor dat het bestuur (B&W) de maatregelen voor informatieveiligheid moeten goedkeuren en toezicht moeten houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen. Het college is geïnformeerd over de komst van de nieuwe wet.[64]

[56] Bron: *Handboek Publieke Zorg*
[57] Bron: *Handboek Teamleider Preparatie Nafase*
[58] Bron: *Handboek Proces Ondersteuning*
[59] Bron: *Regionaal Crisisplan Veiligheidsregio Utrecht*
[60] Een *koude fase* is de voorbereidende periode vóór een crisis of incident. Het doel van deze fase is het opstellen van protocollen en het oefenen van rollen en taken, zodat tijdens een daadwerkelijke crisis (de warme fase) efficiënt kan worden opgetreden.
[61] Bron: *ICT kritieke verstoringen proces v0.3*
[62] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.2.
[63] Bron: Gemeente Stichtse Vecht (2025). *Verkenning Digitale weerbaarheid*, p.2.
[64] Informatieve sessie colllege 2024 – informatiebeveiliging en gegevensbescherming

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

7. De gemeenteraad

De gemeenteraad heeft, net als bij andere domeinen, een kaderstellende en een controlerende rol op het gebied van informatiebeveiliging. Om na te gaan hoe deze rol wordt ingevuld, hebben wij eerst gekeken naar de manier waarop de rol van de gemeenteraad beschreven is in het beleidsplan. Vervolgens hebben wij de informatievoorziening aan de raad onderzocht. Ten slotte hebben wij een gesprek gevoerd met raadsleden van verschillende fracties om na te gaan hoe raadsleden hun rol op dit domein zelf ervaren.
De belangrijkste conclusies uit dit hoofdstuk zijn:

- De gemeenteraad wordt onvoldoende in stelling gebracht om de kaderstellende en controlerende rol op het gebied van informatiebeveiliging goed te vervullen;
- De gemeenteraad wil een actievere en meer sturende rol spelen op dit domein

7.1. Informatievoorziening aan de gemeenteraad

In het beleidsdocument ‘Informatiebeveiligingsbeleid 2020 – 2023’ is een bescheiden rol opgenomen voor de gemeenteraad: ‘Door middel van het hoofdstuk informatieveiligheid in het jaarverslag en de uitkomsten van ENSIA in de collegeverklaringen legt het College verantwoording af aan de gemeenteraad over informatieveiligheid’.

In de praktijk blijken deze documenten nauwelijks informatie te bevatten over het informatiebeveiligingsbeleid en de uitkomsten daarvan. Zo hebben de uitkomsten van ENSIA alleen betrekking op een de beveiliging rond SUWINET en de DigiD-aansluitingen van de gemeente. Dit betreft slechts een klein onderdeel van het gehele IT-landschap van de gemeente.

In de jaarstukken van 2022, 2023 en 2024 wordt in het hoofdstuk ‘Bedrijfsvoering’ een korte paragraaf gewijd aan informatiebeveiliging. Kort worden enkele relevante ontwikkelingen beschreven die betrekking hebben op de gemeentelijke organisatie en wijzigingen in wettelijke kaders. Deze informatie is echter onvoldoende voor de raad om zijn controlerende rol goed uit te voeren. Zo wordt in de jaarstukken van 2022 aangegeven dat ‘Inwoners, ondernemers en medewerkers vertrouwen erop dat wij voldoen aan de wettelijke verplichtingen en normen uit de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO)’. Maar er staat niet of deze verwachtingen ook worden waargemaakt.

In de kadernota 2025 staat met betrekking tot informatiebeveiliging het volgende:
We stellen voor om de volgende ontwikkelingen binnen de bedrijfsvoering (voorlopig) binnen bestaande budgetten op te vangen:
• Voldoen aan (nieuwe) wet- en regelgeving in relatie tot (data)beveiliging en archivering. Een doorontwikkeling van de ICT omgeving gericht op rationalisering applicatielandschap, beweging naar cloudapplicaties en het door ontwikkelen van de kantoorautomatisering. In dat kader is ook een aanbesteding van bedrijfsbrede software noodzakelijk, door het aflopen van bestaande contracten.[65]

In aanvulling op deze formele informatiebronnen wordt de raad ook via werkconferenties en raadsinformatiebrieven geïnformeerd. De laatste werkconferentie heeft op 20 mei 2025 plaatsgevonden en was verzorgd door de CISO en PO. In raadsinformatiebrieven komt het onderwerp niet of nauwelijks aan de orde.

[65] Bron: *Kadernota 2025*, p.12. Geraadpleegd via: https://raadsinformatie.stichtsevecht.nl/Vergaderingen/Commissie-Bestuur-en-Financien/2024/18-juni/19:30/Kadernota-2025/Kadernota-2025-Raad.pdf

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Raadsleden zijn ook gebruiker van gemeentelijke informatie en informatiesystemen. Zij krijgen regelmatig vertrouwelijke informatie waarmee zorgvuldig om moet worden gegaan. Raadsleden (en collegeleden) worden niet standaard meegenomen als doelgroep van de afdeling leren en ontwikkelen. De voor de ambtelijke organisatie verplichte (digitale) trainingen worden dus niet aangeboden aan raadsleden. Ook het gebruik van eigen devices voor gemeentelijke informatie, bijvoorbeeld het doorsturen van mails naar privémailadres, kan een bedreiging vormen voor de informatieveiligheid.

Raadsleden kunnen ook zelf vragen (schriftelijk en mondeling) stellen aan het college. Op het gebied van informatiebeveiliging gebeurt dit nauwelijks. De afgelopen periode zijn twee raadsvragen gesteld op het gebied van digitalisering die zijdelings te maken hadden met digitale veiligheid.

7.2. De rol van de raad volgens de VNG

Volgens de VNG is het belangrijk dat raadsleden invloed uitoefenen op de gemeentelijke informatiebeveiliging ‘door vooraf goede kaders te stellen, regelmatig het thema te agenderen op de raadsagenda en actief het college hierop te controleren. Het vrijmaken van voldoende middelen daartoe is daar één op één mee verbonden. In de begrotings- en verantwoordingsbesprekingen is het raadzaam om daar tijd voor te blijven inruimen.[66]’
De VNG heeft op zijn website een factsheet Raadsleden en informatiebeveiliging en een checklist digitale veiligheid voor raadsleden. In deze documenten zijn de hierboven genoemde sturingsmogelijkheden door de gemeenteraad nader uitgewerkt.

7.3. Uit de raadsbijeenkomst

Als onderdeel van dit onderzoek hebben wij op 25 juni 2025 een raadssessie georganiseerd om op te halen hoe de raadsleden van Stichtse Vecht hun rol op dit domein zelf in (willen) vullen. Bij deze bijeenkomst waren tien raadsleden aanwezig uit verschillende fracties. Zij gaven aan dat informatiebeveiliging als een apart domein gezien moet worden. Dit domein zou een vaste plek moeten krijgen in de P&C-cyclus. In de rapportage aan de raad moeten niet alleen de plannen worden beschreven, maar ook de realisatie ervan en wat de organisatie hiervan geleerd heeft. Deze informatie moet de raad inzicht verschaffen in de mate waarin ‘het eigen huis’ op orde is. Hierbij moet de aandacht niet uitgaan naar de techniek, maar naar de normatiek. De aanwezige raadsleden geven aan dat zij graag willen weten of de gemeente voldoet aan de geldende normenkaders. Ook willen zij inzicht in de risico’s, zodat zij de goede prioriteiten kunnen stellen. Deze informatie moet wel op het goede abstractieniveau worden aangeboden. Zo geven raadsleden aan dat zij niet willen weten wat er in het normenkader staat, maar wel of er aan de normen wordt voldaan. Datzelfde geldt voor de realisatie van het jaarplan; de raad wil weten of de doelen uit het plan gerealiseerd zijn en is niet geïnteresseerd in hoe dat dan gedaan is. Hierbij wordt wel de kanttekening geplaatst dat in geval van calamiteiten wel gedetailleerde informatie gewenst is.

[66] Raadgever Digitale veiligheid op de VNG website: https://vng.nl/artikelen/raadgever-digitale-veiligheid

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

8. Bestuurlijke reactie

t.a.v. Rekenkamer Stichtse Vecht

Datum
18 november 2025
Onderwerp
Bestuurlijke reactie Rekenkameronderzoek

Geachte Rekenkamer,

In deze bestuurlijke reactie reageert het college op uw rapport “Digitale Veiligheid in Stichtse Vecht.” Allereerst dankt het college de Rekenkamer voor het onderzoek en haar bevindingen. We reageren hierbij op uw bevindingen, maar plaatsen onze reactie wel in het licht van de grote ontwikkelingen die onze gemeente op dit punt in de afgelopen jaren heeft gemaakt en het wettelijk kader van de cyberveiligheidswet die waarschijnlijk pas over een half jaar volledig van kracht is.

Samenvatting
De conclusies en aanbevelingen plaatst het college in de context om verder te bouwen aan een toekomstgerichte ambtelijke organisatie voor Stichtse Vecht.

Informatieveiligheid is een onderwerp dat met de toenemende digitalisering steeds belangrijker wordt. Gemeenten verwerken grote hoeveelheden gegevens in een veelvoud aan informatiesystemen. Veel van deze gegevens betreffen (bijzondere) persoonsgegevens of andere belangrijke informatie die goed beschermd moeten zijn.

Naar verwachting treedt in het tweede kwartaal van 2026 de Cyberbeveiligingswet (Cbw) in werking. Hiermee wordt digitale veiligheid een wettelijke verplichting voor gemeenten. Dit betekent dat er extra verplichtingen voor gemeenten gaan gelden op het gebied van de zorgplicht, meldplicht en toezicht. Deze wet is een directe aanleiding voor de Rekenkamer van Stichtse Vecht om dit onderzoek uit te voeren.

In het eindrapport heeft de Rekenkamer conclusies en aanbevelingen opgenomen met betrekking tot de wijze waarop Stichtse Vecht zich heeft voorbereid op dit veranderende wettelijke kader. Graag reageren we eerst op de aanbevelingen. Daarna gaan we in op de conclusies.

Ten aanzien van de aanbevelingen van de Rekenkamer:

1. Aanbeveling 1: Vraag het college om een passend strategisch beleid voor informatiebeveiliging.

   De gemeente laat zich adviseren door de Informatiebeveiligingsdienst (IBD). Het IBD is onderdeel van de VNG en ondersteunt gemeenten bij preventie, detectie, coördinatie en kennisdeling op het gebied van informatiebeveiliging.

   Het IBD past bij belangrijke wijzigingen - zoals de komst van de Cbw - formats voor beleid aan. Omdat er onduidelijkheid was over de ingangsdatum van de Cbw heeft de IBD het format nog niet beschikbaar. De IBD is momenteel bezig met de afronding van het format voor het Informatie-beveiligingsbeleid. Zodra dit gereed is, zal het huidige beleid worden herzien.

   In dit beleid wordt richting gegeven aan het inrichten van informatiebeveiliging en privacy binnen de gemeente. Er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en de middelen waarmee dit beleid moet worden vormgegeven.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Hiermee wordt het Strategisch Informatiebeveiligingsbeleid weer actueel en in lijn met de geldende wet- en regelgeving.

Het college was reeds voornemens om het strategisch beleid aan te passen en kan daarom deze aanbeveling overnemen.

2. Aanbeveling 2: Zorg voor voldoende capaciteit (mensen en middelen) en ambtelijke prioriteit om conform het nieuwe strategisch beleid te werken en aan de wettelijke verplichtingen te voldoen.

   Capaciteitsvraagstukken zijn niet direct aan de raad. Echter het beschikbaar stellen van voldoende middelen voor het uitvoeren van een taak is dat wel. In die zin lezen wij als college deze aanbeveling. Daarbij plaatsen we de kanttekening dat alleen capaciteit niet voldoende is. We moeten namelijk ook voldoende kwaliteit kunnen krijgen uit de markt; die is momenteel zeer schaars aanwezig. Vanzelfsprekend wordt vanuit de ambtelijke organisatie sterk ingezet op dit punt.

   Gelet op het bovenstaande kan het college meegaan in het deel van de aanbeveling om voor voldoende ambtelijke capaciteit te zorgen.

3. Aanbeveling 3: Vraag het college om de raad op korte termijn te informeren over de bestuurlijke risico-afwegingen die de gemeente neemt.

   In het licht van veranderende landelijke wet- en regelgeving wordt er gewerkt aan een manier van rapporteren en controleren, vanuit de plan-do-check-act-gedachte (zie ook het antwoord op aanbeveling 4). Er wordt op het moment beperkt gerapporteerd over de status van de BIO (Baseline Informatiebeveiliging Overheid, basisnormenkader). Het is geen werkend systeem van controle en rapportage over informatiebeveiliging. Hierdoor wordt de plan-do-check-act (PDCA) cyclus nog niet volledig uitgevoerd. Het college is echter wel al op 12 november geïnformeerd over de mate waarin de gemeente voldoet aan de BIO-norm.

   Dat laat onverlet dat er verbeterslagen nodig zijn op het gebied van rapportage, zodat het college een goede bestuurlijke risico-afweging kan maken. Het college zal de raad informeren zodra de verbeterslagen zijn doorgevoerd.

4. Aanbeveling 4: Maak afspraken met het college over welke informatie de gemeenteraad periodiek nodig heeft om te kunnen sturen en controleren.

   Deze aanbeveling heeft overeenkomsten met aanbeveling 3.

   Vooruitlopend op de veranderende landelijke wet- en regelgeving is er een initiatief gestart voor de aanschaf van ISMS tooling (Information Security Management System) ook wel GRC (Governance Risk Compliance) genoemd. Dit heeft als doel het systematisch beheren van beveiligingsrisico's, het identificeren en behandelen van bedreigingen en het implementeren van beheersmaatregelen.

   Een ISMS is zo ingericht dat de bijbehorende activiteiten, processen en documenten samen een plan-do-check-act cyclus vormen die de opzet, inrichting en werking aantoonbaar en controleerbaar maken. Hierdoor beschikt het bestuur over de juiste informatie om weloverwogen besluiten te nemen over informatiebeveiliging en risico's. Het hebben van een ISMS wordt met de invoering van de Cbw verplicht.

   Het college heeft op termijn dus (betere) informatie en rapportage, welke met de raad gedeeld kan worden. We maken graag afspraken met de raad over hoe en wanneer we in de tussentijd aan de raad rapporteren.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Ten aanzien van de conclusies van de Rekenkamer

Digitale infrastructuur
Bevinding Rekenkamer:
Uit het onderzoek blijkt dat de gemeente een inhaalslag heeft gemaakt op het gebied van de digitale infrastructuur. Waar de gemeente eerder zelf een serverpark beheerde, worden applicaties nu naar de cloud verplaatst, waarbij leveranciers verantwoordelijk zijn voor de technische informatiebeveiliging. De gemeente blijft verantwoordelijk voor het voldoen aan wettelijke beveiligingseisen en normen.

Reactie college:
Het college onderschrijft deze conclusie.
De conclusie plaatst het college in de context om verder te bouwen aan een toekomstgerichte ambtelijke organisatie voor Stichtse Vecht.

Beleid en uitvoering
Bevinding Rekenkamer:
Het strategisch beveiligingsbeleid van de gemeente is gebaseerd op een format van de IBD en bevat belangrijke aspecten van informatiebeveiliging, maar is verouderd en houdt geen rekening met recente ontwikkelingen zoals nieuwe wetgeving en toegenomen bedreigingen.

De BIO is de baseline voor informatiebeveiliging en dus de ‘ondergrens’. Stichtse Vecht voldoet nog niet aan deze ondergrens. Hoewel het beleid de BIO als normenkader hanteert en 10 principes voor informatiebeveiliging benoemt, wordt in de praktijk niet altijd conform het beleid gewerkt, met name op het gebied van risicomanagement en bestuurlijke controle. De PDCA cyclus wordt niet effectief toegepast en structurele rapportages ontbreken.

In de interviews worden twee belangrijke oorzaken aangedragen voor het feit dat er niet volgens het eigen beleid gewerkt wordt. De eerste is de bovengenoemde inhaalslag inclusief de migratie naar ‘de Cloud’. De tweede oorzaak is het gebrek aan ambtelijke capaciteit.

Positief is dat medewerkers goed bewust zijn van het belang van informatiebeveiliging en dat er technisch veel aandacht aan wordt besteed. De extra eisen van de Cbw voor gemeenten zijn duidelijk in kaart gebracht, zowel wat betreft de gewenste eindsituatie als de benodigde mensen, middelen en activiteiten.

Reactie college:
Het college onderschrijft deze conclusie.
De gemeente heeft technisch en organisatorisch stappen gezet op het gebied van informatiebeveiliging om bescherming te bieden tegen de voortdurend veranderende kwetsbaarheden en cyberaanvallen. Aandacht en focus voor informatiebeveiliging blijft gezien de toenemende dreigingen hard nodig om continuïteit en vertrouwen in de dienstverlening te borgen. Om informatiebeveiliging naar een hoger niveau te brengen zijn vervolgacties nodig. Hiervoor zijn aandachtsgebieden in beeld en kaart gebracht.

De rol van het bestuur
Bevinding Rekenkamer:
Onder de Cbw verandert de rol van het bestuur, waarbij het college verplicht wordt risicogericht te sturen op informatiebeveiliging en een training te volgen. De Rijksdienst Digitale Infrastructuur (RDI) kan boetes opleggen bij niet-naleving. Momenteel voldoet de sturing van het college niet aan de eisen van de Cbw, omdat besluitvorming niet gebaseerd is op risicomanagement en er geen periodieke rapportages plaatsvinden. Ook de gemeenteraad controleert het college onvoldoende en

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

mist een sturingskader, waardoor zowel de controlerende als kaderstellende rol niet effectief wordt ingevuld. Raadsleden pleiten ervoor om informatiebeveiliging als een volwaardig gemeentelijk domein te beschouwen.

Reactie college:
Het college onderschrijft deze conclusie.
Met de invoering van de Cbw worden er hogere eisen gesteld aan de normen voor informatiebeveiliging en gegevensbescherming. Niet alleen op technisch en organisatorisch gebied, maar ook op naleving. Hierdoor is het van belang om op basis van de juiste informatie weloverwogen besluiten te nemen over informatiebeveiliging en het identificeren en beheersen van risico's. Hierdoor wordt de raad in staat gesteld haar controlerende en kaderstellende rol effectiever te vervullen.

Tenslotte
We danken de Rekenkamer nogmaals voor dit onderzoek en de aanbevelingen. De aanbevelingen sluiten goed aan op de voorbereidingen die het college al in gang heeft gezet om het beleid met betrekking tot informatiebeveiliging aan te scherpen conform nieuwe landelijke wet- en regelgeving. Het college gaat graag met de raad in gesprek omtrent de bevindingen van de Rekenkamer om verder te bouwen aan een stevig fundament voor de digitale veiligheid voor Stichtse Vecht.

Met vriendelijke groet,

Burgemeester en wethouders van Stichtse Vecht,

drs. A.J.H.T.H. Reinders
burgemeester

drs. R.C.L. Heijdra
gemeentesecretaris

gemeente Stichtse Vecht

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

9. Nawoord rekenkamer

De rekenkamer heeft met belangstelling en waardering kennis genomen van de bestuurlijke reactie van het college. Wij constateren dat het college onze conclusies deelt en onze aanbevelingen onderschrijft. We zijn tevens verheugd dat het college voor een zo heldere opzet van het bestuurlijk oordeel heeft gekozen. Daardoor wordt het per aanbeveling en conclusie veel duidelijker wat de reactie van het college daarop is.

Het is goed om te lezen dat er al verschillende stappen worden ondernomen om invulling te geven aan de aanbevelingen. De rekenkamer hoopt met het onderzoek en rapport een bijdrage te hebben geleverd aan de succesvolle invoering van de cyberbeveiligingswet en ziet de behandeling van het rapport door de raad met belangstelling tegemoet.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

Bijlagen

A. DOCUMENTATIE

Document	Datum
Strategisch informatiebeveiligingsbeleid 2020-2023 (versie 1.1)	10 december 2024
Memo Uitstellen actualisering Strategisch Informatiebeveiligingsbeleid, (14 oktober 2024).	14 oktober 2024
Coalitieakkoord 2022-2026 ‘Bouwen aan een stevig fundament voor Stichtse Vecht’	2022
De tien bestuurlijke principes voor informatiebeveiliging, VNG	2019
Jaaropdracht Gegevensbescherming & Informatieveiligheid 2022	10 juni 2022
Verantwoording jaaropdracht Gegevensbescherming & Informatieveiligheid 2022	30 juni 2023
Jaaroverzicht beveiligingsincidenten en datalekken 2022	14 april 2023
DEF Jaaropdracht Gegevensbescherming & Informatieveiligheid 2023	
Jaaroverzicht beveiligingsincidenten en datalekken 2023	5 maart 2024
Jaaroverzicht datalekken 2024	2025
GAP-analyse BIO 2024	2024
Prioritering maatregelen Infra en KA 0.3	2025
Deltaplan ICT en IV	9 juli 2024
Rekenkameronderzoek Risicomanagement in de gemeente Stichtse Vecht	2024
Kadernota 2025	
Bijlage met nadere uitwerking geregistreerde datalekken periode januari t/m december 2024	2024
Protocol meldplicht datalekken	2019
Tactisch logging & monitoring beleid 2025 - 2028	4 april 2025
Basis PVE Aanbesteding	
Stichtse Vecht Verwerkersovereenkomst-v-2.51	
Logische Toegangsbeveiligngsbeleid	4 augustus 2023
Procesdocumentatie: ICT Incident Management	27 november 2023
Vragenlijst informatiebeveiliging en compliance	
Jaarstukken 2022	2023
Jaarstukken 2023	2024
Bedrijfscontinuïteitsbeleid gemeente Stichtse Vecht v1.0	2024
Bedrijfscontinuïteitsplan (BCP) GSV v1.0	2024
BIA Bedrijfsvoering samenleving v1.0	2024
BIA Publiekszaken en dienstverlening v1.0	2024
Diverse BIA’s	
Handboek Publieke Zorg	
Handboek Teamleider Preparatie Nafase	
Handboek Proces Ondersteuning	
Regionaal Crisisplan Veiligheidsregio Utrecht	2023
Protocol meldplicht datalekken	25-6-2025
Rapportage Compliance & leveranciersmanagement	2025

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

B. GESPREKKEN

Rol
Gemeentesecretaris
Portefeuillehouder ICT
Programmamanager ICT Infrastructuur & kantoorinformatisering
Manager data en informatiemanagement
Functionaris gegevensbescherming
Privacy officers (2)
Informatiemanager
CISO
ISO
Adviseurs leren en ontwikkelen (2)
Verschillende medewerkers in de focusgroep

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

C. VERPLICHTINGEN CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet (Cbw) bevat drie verplichtingen, namelijk zorgplicht, meldplicht en registratieplicht. Daarnaast komt er formeel toezicht op de Cbw.

Zorgplicht

De Cyberbeveiligingswet bevat een zorgplicht die organisaties verplicht zelf een risicoanalyse uit te voeren. Op basis daarvan nemen zij passende en evenredige maatregelen voor de beveiliging van hun netwerk- en informatiesystemen. De leden van het bestuur van entiteiten moeten de maatregelen goedkeuren en toezicht houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen.[67]

.

Registratieplicht

De Cyberbeveiligingswet verplicht organisaties die onder de wet vallen om zich te registreren. Dit wordt de registratieplicht genoemd. Er is door het Nationaal Cyber Security Centrum (NCSC) een online registratievoorziening ontwikkeld waarin organisaties zichzelf registreren en aanmelden.[68]

Meldplicht

De richtlijn schrijft voor dat NIS2-organisaties significante incidenten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Er geldt een gefaseerde meldplicht. De eerste melding is een vroegtijdige waarschuwing die binnen 24 uur na waarneming van het incident, plaatsvindt. Het gaat om incidenten die de verlening van de diensten van de organisatie aanzienlijk (kunnen) verstoren. De drempelwaarden voor significante incidenten worden nog nader uitgewerkt. Voorbeelden van factoren die incidenten tot een significant incident maken zijn de omvang van de financiële verliezen voor betrokkenen en/of het veroorzaken van (operationele) schade aan andere entiteiten dan de getroffen entiteit. Voor het doen van meldingen heeft het NCSC een centraal meldpunt ingericht.[69]

Toezicht

Gemeenten vallen in de Cyberbeveiligingswet onder proactief toezicht. Dit wil zeggen dat er toezicht gehouden wordt op het naleven van de verplichtingen uit de Cyberbeveiligingswet, zoals de zorg- en meldplicht, ook wanneer er geen sprake is van eventuele incidenten. De toezichthouder kan beveiligingsaudits en –scans uitvoeren en informatie verzoeken die nodig is om de risicobeheersmaatregelen van de gemeente te beoordelen. Sancties richten zich tot de entiteit maar kunnen in een uiterst geval ook de individuele bestuurders raken.[70]

[67] Informatiebrochure Cyberbeveiligingswet (2024) NCSC.
[68] Informatiebrochure Cyberbeveiligingswet (2024) NCSC.
[69] Informatiebrochure Cyberbeveiligingswet (2024) NCSC.
[70] Informatiebrochure Cyberbeveiligingswet (2024) NCSC.

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

D. BEOORDELING NORMENKADER

Bij aanvang van het onderzoek heeft de rekenkamer een normenkader vastgesteld. Hiervoor zijn de deelvragen als uitgangspunt genomen.
In onderstaande tabel geven wij per norm een beoordeling of de gemeente:

- Geheel voldoet (GROEN)
- Gedeeltelijk voldoet (ORANJE)
- Niet voldoet (ROOD)

	Vraag / Norm	Beoordeling
1	**Wat doet de gemeente Stichtse Vecht op het gebied van informatieveiligheid? *(proces/organisatie)***	
	De gemeente heeft BIO-conform informatiebeveiligingsbeleid.	
	In het beleid wordt o.a. ingegaan op a) strategische uitgangspunten, b) risicomanagement, c) governance (waaronder rollen en verantwoordelijkheden) en de PDCA-cyclus van de gemeente.	
	De gemeente heeft de maatregelen uit de zorgplicht ingeregeld (tien maatregelen).	
	De gemeente heeft aanvullende maatregelen getroffen, onder andere op het gebied van bescherming van persoonsgegevens.	
	Er is een risicoanalyse en beveiliging van de informatiesystemen.	
	Er is beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen.	
	De gemeente informeert belanghebbenden over datalekken en incidenten	
2	**Hoe bevordert de gemeente het bewust omgaan met informatie? *(mens)***	
	De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging. Ze krijgen informatie over wijzigingen.	
	Er is sprake van cyberhygiëne en er worden trainingen aangeboden en gevolgd op het gebied van cyberbeveiliging	
	De medewerkers gebruiken multi-factor-authenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen.	
	In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven.	
	De gemeente monitort actief op het naleven van veilig werken.	
	De gemeente evalueert na informatiebeveiligingsincidenten en datalekken.	
3	**Zijn gegevens bij de gemeente goed beschermd tegen de toegang door onbevoegden? *(techniek)***	
	Er zijn beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets.	

gemeente Stichtse Vecht

Endelhovenlaan 1, 3601 GR Maarssen
Postbus 1212, 3600 BE Maarssen
T 140346 **F** 0346 25 40 10

info@stichtsevecht.nl

	Er is beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden.	
	De gemeente heeft een risico-afweging gemaakt bij de bescherming van de systemen, waarbij de gevolgen voor burgers en bedrijven in beeld zijn.	
	De gemeente weet welke risico's zij loopt en op de hoogte van mogelijke kwetsbaarheden. Daarover is een afweging gemaakt in relatie tot gevoelige informatie.	
	De gemeente voert penetratietesten uit.	
	Incidenten en onderzoeken op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.	
	De gemeente heeft de logging van gegevens ingeregeld en hierbij een afweging gemaakt op basis van risicoanalyse.	
	De gemeente heeft autorisatiebeleid ingeregeld en zorgt ervoor dat dit up-to-date wordt gehouden.	
4	**Welke (verdere) maatregelen zijn mogelijk om de informatieveiligheid te optimaliseren?**	
	De gemeente heeft een beeld bij de overige verplichtingen uit de cyberbeveiligingswet, namelijk de meldplicht en toezicht.	
	De gemeente treft voorbereidingen om te voldoen aan de Cyberbeveiligingswet.	
	De gemeente toetst, oefent en evalueert maatregelen/acties/processen periodiek (zoals het oefenen van een cyberaanval).	
	De rollen en verantwoordelijkheden van functionarissen, directie en raad zijn vastgelegd en in de praktijk bekend.	
5	**Hoe is de raad betrokken bij (de uitvoering van) het beleid ten aanzien van de informatieveiligheid?**	
	De raad wordt structureel en regelmatig geïnformeerd over het beleid en de uitvoering rondom informatieveiligheid. De raad wordt geïnformeerd over risico's, maatregelen en ontwikkelingen.	
	De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.	
	De raad is aantoonbaar betrokken bij het bepalen van de uitgangspunten en kaders van het informatieveiligheidsbeleid.	
	De raad is aantoonbaar actief in het controleren en beoordelen van het informatieveiligheidsbeleid.	