Gemeente Zeist

GEMEENTEBLAD

Officiële uitgave van de gemeente Zeist

Nr. 533266

14 december

2023

Strategisch Informatieveiligheidsbeleid Gemeente Zeist 2022-2026

1. Inleiding

Deze beleidsnota beschrijft het strategisch Informatieveiligheidsbeleid voor de jaren 2022 - 2026 en vervangt het in 2019 vastgestelde '*Strategisch Informatieveiligheidsbeleid Weerbaar verder*'.
Met dit 'Strategisch Informatieveiligheidsbeleid' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn.

De nota is richtinggevend en kaderstellend en wordt aangevuld met specifieke beleidsdocumenten voor Informatieveiligheid op tactisch niveau en werkinstructies op operationeel niveau.
De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatieveiligheid Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor Informatieveiligheid zoals uitgewerkt door de VNG (zie 3.2.2)[1] .

1.1. Leeswijzer

In het eerste hoofdstuk wordt de ambitie en visie van de gemeente beschreven. Hoofdstuk 2 gaat in op de ontwikkelingen op het gebied van Informatieveiligheid in Nederland en daarbuiten. In het daarop volgende hoofdstuk wordt de kern van het strategisch beleid uiteengezet. Hoofdstuk 4 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

Dit beleid is door het College van B&W vastgesteld voor de periode van 2022-2026. Uiterlijk het laatste jaar zal het geëvalueerd, waar nodig aangepast en opnieuw vastgesteld worden. Indien een nieuw beleidskader binnen deze termijn nog niet is vastgesteld, dan blijft het huidige beleidskader tot dat moment van toepassing.

1.2. Wat is Informatieveiligheid?

Onder Informatieveiligheid wordt verstaan het treffen en onderhouden van een samenhangend pakket van beheersingsmaatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Hieronder vallen alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en gegevens(verzamelingen). Kernpunten daarbij zijn:

- **B**eschikbaarheid / continuïteit: zorgen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- **I**ntegriteit / betrouwbaarheid: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- **V**ertrouwelijkheid / exclusiviteit: beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Het Informatieveiligheidsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen of procesautomatiseringssystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT, maar overstijgt afdelingsgrenzen en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3. Ambitie en visie op Informatieveiligheid

De gemeente voert een belangrijke en omvangrijke set publieke taken uit, die zijn verankerd in wet- en regelgeving. Daarvoor verwerken we veel (gevoelige) informatie van burgers en organisaties. Zij verwachten terecht dat wij zorgvuldig met die informatie omgaan en die beschermen. Continuïteit en betrouwbaarheid zijn essentieel voor de werking van onze samenleving en het vertrouwen daarin. De groeiende dreiging van incidenten en crises voedt het risico op grote maatschappelijke en politieke gevolgen.

De ontwikkelingen qua dreigingen op het gebied van Informatieveiligheid en daadwerkelijke gevolgen, zoals Hof van Twente, zijn alarmerend. Incidenten die in het nieuws komen hebben ernstige gevolgen, zowel financieel als voor het vertrouwen in de overheid. En dat terwijl digitalisering cruciaal is voor het behalen van de doelen van de gemeente en hand in hand gaat met een goed en betrouwbaar functionerende informatievoorziening.

1) De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf (informatiebeveiligingsdienst.nl)

De gemeente moet borgen dat het (gehele) proces en de daarbij behorende informatie onder alle omstandigheden beschikbaar, tijdig, juist, volledig en alleen toegankelijk voor de juiste personen is. Mocht er toch iets misgaan moet dit snel worden opgemerkt en herstelbaar zijn.
Het sterk toenemende dreigingsniveau heeft een immense impact op het omgaan met digitale weerbaarheid. Gevaren verdwijnen niet, maar nemen juist toe en veranderen steeds. Het realiseren van Informatieveiligheid is niet iets wat je eenmalig doet. Voortdurend verbeteren is belangrijk. Het belang en de afhankelijkheid van veilige IT-voorzieningen nemen toe, net als toenemende technologische mogelijkheden en bedreigingen op dit gebied.

Om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie blijvend te waarborgen is het noodzakelijk om op het gebied van Informatieveiligheid te groeien. Als volwassenheidsmodel hanteren we het model dat door de NBA-LIO (Nederlandse Beroepsorganisatie voor Accountants – Ledengroep Intern en Overheidsaccountants), met medewerking van NOREA (de beroepsorganisatie van IT-Auditors) is opgesteld. Het wisselt per proces op welk volwassenheidsniveau wordt geacteerd. Het helpt om tot een reëel ambitieniveau te komen, passend bij de risicobereidheid en beschikbare capaciteit en middelen. Als team Veilig werken binnen afdeling IV gebruiken we dit model in onze evaluatie en het opstellen van het jaarplan.

Volwassenheids-niveau	Naam	Omschrijving
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.

2. Informatieveiligheid in breder perspectief

Met de toenemende digitalisering wordt het beveiligen van informatie een steeds belangrijker thema. Niet alleen binnen Nederland, maar ook daarbuiten.

2.1. Europese beleidsontwikkelingen

Op alle beleidsniveaus wordt in toenemende mate aan digitale veiligheid gewerkt. Zo wordt in EU-verband gewerkt aan een nieuwe "*EU strategie inzake cyberbeveiliging voor het digitale tijdperk*":

- Daarbij is veel aandacht voor het opzetten van netwerken en operationele samenwerking gericht op o.a. verhogen veerkracht, informatiedeling, veilige next-generatie digitale infrastructuur & technologie, certificering van hard- & software, de stabiliteit van het internet, het trainen van de beroepsbevolking en cyberdiplomatie.
- Deze strategie zal de basis leggen voor nieuwe regelgeving en de actualisatie van bestaande EU-regelgeving, zoals de Cyber Security Act en de Network & Information Security Directive (NIS en NIS2). Heeft vooral impact omdat organisaties als MKB en gemeenten hierin als zijnde vitaal worden gekenmerkt en daarmee voortaan door het NCSC (National Cyber Security Center) worden bediend.

2.2. Nederlandse beleidsontwikkelingen

In *nationaal* verband wordt door de Rijksoverheid verder gewerkt aan de uitwerking van voornoemde EU-regelgeving, o.a. de Wet beveiliging netwerk- en informatiesystemen (Wbni) en de roadmap veilige hard- & software, het bestaande beleid (NCSA) en mogelijke nieuwe investeringen door het nieuwe kabinet. Wat betreft laatstgenoemde zijn de volgende zaken relevant:

- In de brede maatschappelijke heroverwegingen (BMH) is in 2021 voorgesteld dat het kabinet extra investeert in het verhogen van de weerbaarheid van vitale processen (vaak ook "vitale infrastructuur" genoemd) en een minister Digitale Zaken. Dit heeft zich onder andere vertaald in een

staatssecretaris Digitalisering. De ambitie van het digitaliseringsbeleid van het kabinet is een veilige, inclusieve en kansrijke digitale samenleving, waarbij publieke waarden en de gebruikers centraal staan[2].
- De Nederlandse vitale infrastructuur wordt gevormd door processen (zoals bijvoorbeeld telecom en energie) die zo vitaal zijn voor het functioneren van de samenleving, dat verstoring ervan leidt tot instabiliteit en discontinuïteit. De Rijksoverheid kijkt alleen naar de vitale processen die van nationaal belang zijn en heeft hiervoor criteria opgesteld. Dat leidt ertoe dat sommige processen en infrastructuur die op lokaal niveau vitaal zijn voor het functioneren van de stad, zoals ziekenhuizen en scholen, op nationaal niveau niet vitaal zijn en dus ook geen cybersecurity ondersteuning krijgen van het Rijk (via het NCSC).
- Het huidige kabinet heeft €95 miljoen extra geïnvesteerd in cybersecurity. Deze middelen zijn vooral geïnvesteerd in meer personele capaciteit bij verschillende overheidsonderdelen. Het NCSC schaart de gemeente niet onder vitaal en verwijst naar de Informatieveiligheidsdienst (IBD) van de VNG. De samenwerking tussen IBD en het NCSC is de laatste jaren versterkt.
- Bij Business Continuity Management (BCM) ligt de focus vooral op vitale infrastructuur en internationale normen & standaarden. We zien ook een toename van aandacht voor de bestrijding van cybercriminaliteit en gedigitaliseerde criminaliteit.
- De Cyber Security Raad (CSR) adviseert dat organisaties 10% van hun ICT-budget dienen te investeren in cybersecurity. Er zijn echter maar weinig organisaties die aan dit percentage voldoen. Naar dit advies wordt ook verwezen in de resolutie Digitale Veiligheid van de VNG.

2.3. Nederlandse Cybersecurity Agenda (NCSA)
De Rijksoverheid heeft de NCSA opgesteld met als doel dat Nederland in staat is om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen. Deze agenda heeft landelijke impact, maar is niet afgestemd op de agenda's van gemeenten. De NCSA bevat zeven ambities:

- Slagkracht op orde
- internationale vrede & veiligheid in het digitale domein
- veilige hard- en software
- weerbare digitale processen en een robuuste infrastructuur
- succesvolle barrières tegen cybercrime
- kennisontwikkeling
- publiek-private aanpak van cybersecurity.

Eén van de prioriteiten van de NCSA is de vorming van een Landelijk Dekkend Stelsel (LDS) dat ervoor moet zorgen dat (op termijn) een stelsel van cybersecurity samenwerkingsverbanden tot stand komt waarin informatie over cybersecurity breder, efficiënter en effectiever kan worden gedeeld tussen publieke en private partijen.
Ook het jaarlijkse Cybersecuritybeeld Nederland (CSBN), is gekoppeld aan de NCSA en wordt ieder jaar gepubliceerd door de Nationale Coördinator Terrorismebestrijding & Veiligheid (NCTV).

2.4. Agenda Digitale Veiligheid 2020-2024
Het bestuur van de Vereniging Nederlandse Gemeenten (VNG) heeft het thema digitale veiligheid omarmd en begin 2020 in de Agenda Digitale Veiligheid voor gemeenten drie categorieën gedefinieerd.
- eigen Informatieveiligheid op orde;
- digitale criminaliteit;
- digitale incidenten en -crises.

Kernwoorden in de agenda zijn: ketenverantwoordelijkheid, risicomanagement en het aansluiten bij bestaande structuren.

In 2021 hebben de VNG leden ingestemd met de resolutie Digitale Veiligheid, waarin digitale veiligheid een kerntaak van de gemeente wordt genoemd. De resolutie komt voort uit de Agenda Digitale Veiligheid gemeenten 2020-2024. Gemeenten onderschrijven middels de resolutie dat de digitalisering in de samenleving doorzet en dat hiermee naast kansen en mogelijkheden ook risico's toenemen. Gemeenten dragen en voelen de verantwoordelijkheid om continu te werken aan een veilige en weerbare digitale samenleving.

3. Strategisch Informatieveiligheidsbeleid gemeente Zeist
3.1. Doel
Informatieveiligheid is geen doel op zichzelf, maar moet eraan bijdragen dat de gemeente haar ambities, doelen en resultaten (duurzaam) realiseert. De informatie die Zeist verwerkt is in beginsel van en voor

2) Kamerbrief hoofdlijnen beleid voor digitalisering - Digitale Overheid

burgers, bedrijven en bezoekers van Zeist. Het doel van de gemeentelijke informatievoorziening is het vervullen van haar taken en het daarbij bieden van diensten aan inwoners en organisaties, in toenemende mate via de digitale weg. Het daarvan afgeleide organisatiedoel ten aanzien van informatieveiligheid is het waarborgen van de continuïteit, integriteit en vertrouwelijkheid van de informatievoorziening.

3.2. Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het informatieveiligheidsbeleid zijn:

3.2.1. De BIO
De BIO (Baseline Informatieveiligheid Overheid) is sinds 2020 het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de lijnmanagers nu meer dan voorheen moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid. We werken risico-gestuurd, dat wil enerzijds zeggen dat er in de uitvoering voorrang wordt gegeven aan het afwenden van de grootste risico's. Anderzijds wil dit zeggen dat maatregelen niet altijd integraal voor de hele organisatie worden geïmplementeerd, maar dat ook dit risico-gestuurd wordt gedaan. We implementeren maatregelen die passen bij het gewenste risicoprofiel.

3.2.2. De 10 bestuurlijke principes voor Informatieveiligheid
We hanteren de door de VNG opgestelde 10 bestuurlijke principes voor Informatieveiligheid, deze principes zijn een bestuurlijke aanvulling op het BIO normenkader en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatieveiligheid is van iedereen.
3. Informatieveiligheid is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatieveiligheid behoeft ook aandacht in (keten)samenwerking.
6. Informatieveiligheid is een proces.
7. Informatieveiligheid kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van Informatieveiligheid in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement.
Als er iets verkeerd gaat met betrekking tot het beveiligen van informatie binnen de gemeentelijke processen, kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatieveiligheid nadrukkelijk gewenst op de bestuurstafel.

3.2.3. Dreigingsbeeld Informatieveiligheid Nederlandse Gemeenten
De Informatieveiligheidsdienst (IBD) brengt eens in de twee jaar het Dreigingsbeeld Informatieveiligheid Nederlandse Gemeenten uit IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf (Informatieveiligheidsdienst.nl). Dit document geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Een groeiende dreiging van ransomwareaanvallen met als gevolg uitval van, en fouten in de dienstverlening en bedrijfsvoering, vertrouwelijke informatie die in verkeerde handen terechtkomt en reputatieschade met als mogelijk gevolg minder vertrouwen in de overheid.
Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor Informatieveiligheid.

3.2.4. Informatie uit incidenten en inbreuken op de beveiliging
De gemeente kent naast het hierboven genoemde dreigingsbeeld ook een eigen registratie waarin incidenten worden vastgelegd. Dit geeft waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid. Het blijvend evalueren en leren is hierbij het uitgangspunt.

3.2.5. Sourcing
Wij doen steeds minder zelf qua informatieverwerking, veelal omdat de markt die kant op blijft gaan, deels omdat we de kennis niet meer in huis hebben qua beheer. Nieuwe informatiesystemen worden als SaaS afgenomen. De kans op - en impact van grote verstoringen neemt door die fragmentering af, het risico moet per geval bekeken en beheerst worden (vergt tactische inzet, competenties en rollen

Wij kunnen 24/7 monitoring en respons die vereist is (o.a. SIEM-SOC) onmogelijk met eigen middelen klaarspelen. We worden dus ook daarin afhankelijk van marktpartijen en intern vergt die vooral een professionele regie-organisatie en bijvoorbeeld piket dienst.
Ook infrastructuur (datacenter en netwerk) zit in deze trend; dit laten we door externen beheren en veelal ook niet meer op onze locatie draaien. Daarmee ook de maatregelen qua beveiliging, die gaan daarmee ook naar externe partijen. Het voeren van regie blijft hierbij essentieel.

3.3. Standaarden Informatieveiligheid
De basis voor inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden genomen op basis van best practices bij (lokale) overheden en genoemde norm.
Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun Informatieveiligheidsbeleid heeft de interbestuurlijke werkgroep Normatiek[3] in 2018 de Baseline Informatieveiligheid Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

3.4. Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van Informatieveiligheid op tactisch en operationeel niveau. Deze nota beschrijft op strategisch niveau het Informatieveiligheidsbeleid. Dit beleid wordt op tactisch niveau aangevuld met specifieke beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatieveiligheidsplan worden deze tactische en operationele aspecten van Informatieveiligheid verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de lijnmanagers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is vastgelegd.

3.5. Scope Informatieveiligheid
De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, technische infrastructuur, procesautomatisering, informatie en gegevens van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch gemeentelijke Informatieveiligheidsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), Paspoorten Nederlandse Identiteitskaarten (PNIK) en Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

Informatieveiligheid en privacy zijn nauwverwante thema's, daar waar Informatieveiligheid alle typen informatie betreft gaat privacy specifiek over persoonsgegevens en het naleven van regels voor de verwerking van persoonsgegevens. Een privacy incident is daarmee altijd ook een Informatieveiligheids incident, maar andersom hoeft dit niet zo te zijn. Zeist heeft separaat beleid inzake bescherming persoonsgegevens (Strategisch Privacy beleid gemeente Zeist 2022-2026.
Op tactisch en operationeel niveau wordt binnen de 2de lijn samengewerkt door de Informatieveiligheid – en privacyfunctionarissen. Dit uit zich onder andere in de samenstelling van het team Veilig werken. Onder leiding van de CIO (hoofd IV) maken de CISO, Strategisch ICT adviseur, TISO, Privacyofficer en optioneel de FG deel dit van dit team. De samenwerking wordt ook tot uiting gebracht doordat de jaarplannen op het gebied van Informatieveiligheid en privacy op elkaar worden afgestemd.

3.6. Uitgangspunten
Het bestuur, het GMT en lijnmanagers spelen een cruciale rol bij het uitvoeren van dit strategische Informatieveiligheidsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.
Op basis hiervan zet het management dit beleid voor Informatieveiligheid op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het GMT geeft een duidelijke richting aan Informatieveiligheid en demonstreert dat zij Informatieveiligheid ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een Informatie-

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

veiligheidsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en gegevens(verzamelingen). Het Informatieveiligheidsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

3.6.1. Strategische doelen

De strategische doelen van het Informatieveiligheidsbeleid zijn:

- het managen van de Informatieveiligheid;
- 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;
- transparantie over incidenten;
- het waarborgen van de naleving van dit beleid.

3.6.2. Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de Informatieveiligheid en legt hierover verantwoording af aan de gemeenteraad.
- Alle proces automatiseringssystemen die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen vallen binnen de scope van voorliggend beleid.
- Alles wat wij uitbesteden valt onder onze verantwoordelijkheid.
- De uitvoering van Informatieveiligheid is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie en processen die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie en processen ligt dan ook bij de (proces)eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het Informatieveiligheidsbeleid vormt samen met het Informatieveiligheidsplan het fundament onder een betrouwbare informatievoorziening. In het Informatieveiligheidsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatieveiligheid is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van Informatieveiligheid.
- 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.

3.6.3. Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch Informatieveiligheidsbeleid en het jaarlijks op te stellen Informatieveiligheidsplan vast.
- Het GMT is verantwoordelijk voor het laten uitvoeren van het door het college vastgestelde Informatieveiligheidsplan.
- Het GMT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het GMT is verantwoordelijk voor het vragen om informatie bij de lijnmanagers en ziet erop toe dat de lijnmanagers adequate maatregelen genomen hebben voor de bescherming van de infor-

matie, informatiesystemen en proces automatiseringssystemen die onder hun verantwoordelijkheid vallen.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de Informatieveiligheid. De onderwerpen, die als risicovol worden gezien, worden opgenomen in (audit)plannen.
- De lijnmanagers zijn verantwoordelijk voor de uitvoering van Informatieveiligheid van de processen waarvoor zij verantwoordelijk zijn.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Lijnmanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. (lijn)managers zijn verantwoordelijk voor het uitvoeren van quickscans Informatieveiligheid op basis van de BIO om deze risico-afwegingen te kunnen maken.

3.6.4. Plan Do check Act

Informatieveiligheid is geen eenmalige activiteit maar een continu verbeterproces. Dit plan is slechts een enkele stap in een (reeds gestarte) cyclus die steeds opnieuw doorlopen wordt. De kwaliteitscyclus bestaat uit de volgende vier stappen:
- **Plan:** De cyclus begint met het beveiligingsbeleid, gebaseerd op wet- en regelgeving, normenkaders en beleid. Planning gebeurt jaarlijks en wordt vastgelegd in jaarplannen (generiek dan wel specifiek voor een afdeling of taakveld).
- **Do:** Op basis van het beleid en jaarplan worden beveiligingsmaatregelen geïmplementeerd. Uitvoering van beveiligingsmaatregelen maakt integraal onderdeel uit van het werkproces.
- **Check:** Control(e) is onderdeel van het werkproces met als doel: het waarborgen van de kwaliteit van de informatievoorziening en voldoen aan wet- en regelgeving. Jaarlijks worden er bovendien diverse onderzoeken uitgevoerd om opzet, bestaan en/of werking van beveiligingsmaatregelen te toetsen.
- **Act:** Met het opstellen en uitvoeren van verbetervoorstellen is de cyclus rond en start een nieuwe cyclus. Bevindingen van de controles en onderzoeken zijn input voor een nieuw plan.

De gemeente volgt een aanpak van Informatieveiligheid op basis van risicobeheersing. Het streven naar 100% veiligheid is een utopie. Met een aanpak gebaseerd op risicobeheersing is de gemeente beter in staat om een evenwichtige set van veiligheidsmaatregelen te implementeren en om daarbij een betere afweging tussen kosten en noodzaak te maken.
Het startpunt is het uitvoeren van een nulmeting (GAP analyse) op basis van de BIO en bedoeld om inzicht te krijgen in het 'GAP' tussen datgene wat nodig is en wat ontbreekt. Op basis van dat inzicht vindt een impactanalyse plaats waardoor de gemeente in staat is om prioritering te geven aan verbeterpunten voor de korte (denk aan 'Quick Wins') en lange termijn. Bij deze benadering is ruimte voor afweging en prioritering op basis van het principe 'pas toe of leg uit'.
Indien een gemeentelijk proces meer beheersingsmaatregelen nodig heeft dan vindt hierop een (uitgebreide) risicoanalyse plaats. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van het werkproces en de dreigingen die kunnen leiden tot een veiligheidsincident.

3.6.5. Randvoorwaarden

Belangrijke randvoorwaarden zijn:
- We maken afspraken met ketenpartners over Informatieveiligheid zodat beschikbaarheid, integriteit en vertrouwelijkheid van informatie ook daar is geborgd.
- We maken afspraken met (SAAS)leveranciers zodat beschikbaarheid, integriteit en vertrouwelijkheid van informatie ook daar is geborgd.
- We vergroten actief de kennis en het bewustzijn over Informatieveiligheid en omgaan met persoonsgegevens binnen de organisatie.
- Het verder beleggen en borgen van de governance binnen de organisatie.
- Jaarlijks wordt een werkplan veilig werken opgesteld onder leiding van de CIO, gebaseerd op:
  - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - het dreigingsbeeld gemeenten van de IBD;
  - resultaten van risicoanalyse;
  - de door de lijnmanagers ingebrachte onderwerpen.

4. Organisatie, taken en verantwoordelijkheden.

Het college van B&W is bestuurlijk verantwoordelijk voor de veiligheid van informatie binnen de werkprocessen van de gemeente en stelt beleidskaders op voor Informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college van B&W stelt formeel het Informatieveiligheidsbeleid vast, delegeert de uitvoering hiervan aan het hoofd van de afdeling Informatievoorziening (CIO), en informeert jaarlijks de raad over dit thema.
Binnen het college van B&W valt Informatieveiligheid onder de portefeuille van de bestuurder Informatievoorziening. De CISO heeft een onafhankelijke rol en adviseert het college van B&W over het vast te stellen beleid en rapporteert gevraagd en ongevraagd over Informatieveiligheid.

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot Informatieveiligheid op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD)[4]. In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, security officer, privacy officer) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne of externe) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Tabel verantwoordelijken (RASCI) en 3-lijnen model (Three Lines of Defence (3LoD)).[5]

RASCI	3 LoD	Rolverdeling
R – Responsible (operationeel verantwoordelijk)	1ste lijn	• Proceseigenaren / Lijnmanagement • Medewerkers • Uitvoeringsorganisaties (‘verwerkers’)
A Accountable (bestuurlijk eindverantwoordelijk)	1ste lijn	• Het college (verwerkingsverantwoordelijke)
S Supportive (ondersteunend)	2de lijn	• Team Veilig werken, ICT, informatieveiligheid, Inkoop, JZ, risk en kwaliteit management
C Consulted /Toezicht lemand die geraadpleegd wordt	3de lijn	• FG (i.s.m. audit)
I *Informed iemand die geïnformeerd wordt*	*4e lijn*	• *Inwoners, De raad; Accountant;* • *Autoriteit Persoonsgegevens (AP)*

4.1. Aansturing: GMT

Het GMT zorgt samen met het hoofd van de afdeling Informatievoorziening (Chief Information Officer ofwel CIO) dat alle processen en systemen onder verantwoordelijkheid vallen van een lijnmanager. En dat lijnmanagers zich verantwoorden over de beveiliging van de informatie en processen die onder hen berust. Het GMT zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatieveiligheid een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het GMT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. En draagt zorg voor het uitwerken van tactische informatiebeveiligings onderwerpen en laat zich hierin bijstaan door de CISO van de gemeente. Het GMT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatieveiligheid wordt gezien als een integraal onderdeel van risicomanagement.

4.2. Uitvoering: Lijnmanagement / Proceseigenaar

Informatiebeveiliging valt onder de verantwoordelijkheden van alle lijnmanagers en proceseigenaren. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet overdragen, uitvoerende werkzaamheden wel. Vanuit de BIO en rechtmatigheid is de insteek dat alle processen, systemen, data, applicaties altijd minimaal

4) *Het Three Lines of Defense model (3LoD) wordt gebruikt om organisaties in te richten qua governance en control.*
5) *RASCI is de afkorting van Responsible (verantwoordelijke), Accountable (eindverantwoordelijk), Supportive (ondersteunend), Consulted (iemand die geraadpleegd moet worden) en Informed (iemand die geïnformeerd moet worden).*

één eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Lijnmanagers rapporteren aan het GMT over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp Informatieveiligheid te bespreken in het BMO.

Verantwoordelijkheden van de (lijn)managers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
- Het binnen het eigen team uitdragen van het beveiligingsbeleid en daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

4.3. Control en verantwoording
Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van de gemeente. Waarbij zowel de bestuurder als het GMT van gemeente Zeist volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
Het GMT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. En rapporteert over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

4.3.1. ENSIA
De gemeente verantwoordt zich over Informatieveiligheid middels de ENSIA-systematiek. De ENSIA-coördinator is verantwoordelijk voor de coördinatie van dit proces. En zorgt ervoor dat de informatie die nodig is voor het beantwoorden van de ENSIA vragen wordt opgehaald bij de verantwoordelijke (lijn)managers. De (lijn)managers leveren de informatie voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de Informatieveiligheid komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatieveiligheid. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatieveiligheid. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De door de organisatie ingevulde zelfevaluatievragenlijst vanuit de ENSIA vormt de basis voor het opstellen van de collegeverklaring aan de raad. Met deze verklaring geeft het college aan in hoeverre de gemeente voldoet aan de voor DigiD en Suwinet geselecteerde informatiebeveiligings-normen op basis van de Eenduidige Normatiek Single Information Audit ENSIA) systematiek.

De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Informatieveiligheid serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

5. Begrippenlijst

- *Informatieveiligheid:* samenhangend stelsel van beheersingsmaatregelen dat de beschikbaarheid / continuïteit, de integriteit / betrouwbaarheid en vertrouwelijkheid / exclusiviteit van de informatie garandeert (BIV).
- *Beschikbaarheid / continuïteit:* zorgen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *Integriteit / betrouwbaarheid:* waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- *Vertrouwelijkheid / exclusiviteit:* beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.
    - CIO Chief Information Officer
    - CISO: Chief Information Security Officer
    - TISO: Technical Information Security Officer (TISO)
    - PO: Privacy Officer
    - PJ: Privacy Jurist
    - FG: Functionaris voor de Gegevensbescherming: FG
    - AVG: Algemene Verordening Gegevensbescherming
    - WPG: Wet Bescherming Politie Gegevens

- GDPR: General Data Protection Regulation: GDPR
- WBP: Wet Bescherming persoonsgegevens
- IBD: Informatieveiligheidsdienst Nederlandse Gemeenten (IBD).
- ACIB: Algemene Contactpersoon Informatieveiligheid
- VCIB: Vertrouwde Contactpersoon Informatieveiligheid.
- ISMS: Information Security Management System
- ENSIA: Eenduidige Normatiek Single Information Audit
- BIG: Baseline Informatieveiligheid Nederlandse Gemeenten (BIG)
- BIO: Baseline Informatieveiligheid Overheid)
- Suwinet: Digitale infrastructuur voor uitwisseling tussen suwipartijen van gegevens
- BAG: Basisregistratie Adressen en Gebouwen
- BGR: Basisregistratie Grootschalige Topografie
- BRO: Basisregistratie Ondergrond BRO
- BRP: Basisregistratie Personen BRP
- PUN2001: Paspoortuitvoeringsregeling Nederland 2001
- DigiD: Digitale Identiteit
- RBA: Role based acces
- PDCA cyclus: Plan-Do-Check-Act cyclus