

Strategisch informatiebeveiligingsbeleid 2023-2026



Documentbeheer

Versiebeheer

Versie	Datum	Beschrijving
2015	01-07-2015	Eerste versie
2016	21-03-2016	Gewijzigde opzet en indeling i.v.m. een betere aansluiting bij de Baseline Informatiebeveiliging Nederlandse Gemeenten
2017-2019	13-10-2017	Geheel vernieuwde opzet i.v.m. de lengte van het document en aangepast i.v.m. vertrek directeur Bedrijfsvoering.
2020-2022	17-12-2019	Nieuwe versie op basis de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (B1O).
2023-2026	06-09-2023	Nieuwe versie aangepast aan de nieuwe organisatiestructuur
		.

Inwerkingtreding

Dit informatiebeveiligingsbeleid treedt met terugwerkende kracht in werking op 01-01-2023. Het Informatiebeveiligingsbeleid 2020-2022 komt daarmee te vervallen.

Actualisering

De omstandigheden (bedreigingen, technieken, wet- en regelgeving) veranderen voortdurend. Dit informatiebeveiligingsbeleid wordt minimaal na 4 jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.



1. Inleiding.....	3
1.1 Leeswijzer	4
1.2 Wat is informatiebeveiliging?	4
1.3 Ambitie en visie van de gemeente op het gebied van informatieveiligheid.....	4
2. Strategisch beleid	4
2.1 Doel.....	5
2.2 Ontwikkelingen.....	5
2.2.1 De BIO	5
2.2.2 De 10 principes voor informatiebeveiliging	5
2.2.3 Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten	5
2.2.4 Informatie uit incidenten en inbreuken op de beveiliging	5
2.3 Standaarden informatiebeveiliging.....	5
2.4 Plaats van het strategisch beleid	6
2.5 De reikwijdte van informatiebeveiliging	6
2.6 Uitgangspunten.....	6
2.6.1 Strategische doelen	6
2.6.2 Belangrijkste uitgangspunten	7
2.6.3 Invulling van de uitgangspunten	7
2.6.4 Randvoorwaarden.....	8
3. Organisatie, taken & verantwoordelijkheden	8
3.1 Aansturing: directieteam	9
3.2 Uitvoering: teammanagers.....	9
3.3 Controle en verantwoording.....	9
3.3.1 ENSIA	9



1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 tot en met 2026 en vervangt het in 2019 vastgestelde 'Informatiebeveiligingsbeleid 2020-2022'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met specifieke beleidsdocumenten voor informatiebeveiliging 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 Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerpspecifieke beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen informatiebeveiligingsplan, vastgesteld door de directie, worden de beleidsregels verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teammanagers, 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 het beleid. Hoofdstuk 3 beschrijft hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

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

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

Gemeente Krimpenerwaard wil de informatie van inwoners, bedrijven en instellingen die wordt verwerkt zo goed mogelijk beschermen door "passende" beveiligingsniveaus. Er moet evenwicht zijn in de kosten, de stand van de techniek en de risico's die daarbij worden gelopen.

Informatieveiligheid draagt bij aan het realiseren van de ambities en doelen uit het coalitieakkoord. Een veilige informatievoorziening en informatiestructuur maakt het mogelijk de dienstverlening aan inwoners en bedrijven te optimaliseren.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT! Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.



2. Strategisch beleid

2.1 Doel

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2023 tot en met 2026. De uitwerking van dit beleid in beleidsdocumenten op tactisch niveau en concrete maatregelen en werkinstructies op operationeel niveau vindt plaats in het jaarlijks vast te stellen informatiebeveiligingsplan.

2.2 Ontwikkelingen

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

2.2.1 De BIO

De BIO is het normenkader voor de gehele overheid. De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat de teammanagers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

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

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

2.2.3 Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

Het Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek in 2018 de Baseline Informatiebeveiliging Overheid (BIO)



uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook worden praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

2.4 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.

Dit document beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid wordt vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks op te stellen informatiebeveiligingsplan.

2.5 De reikwijdte van informatiebeveiliging

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

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), Paspoorten en Nederlandse identiteitskaarten (PNIK/PUN), Digitale Identiteit (DigiD) 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.

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.
- Alle Proces Automatiseringssystemen (PA) 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.

2.6 Uitgangspunten

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

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.



- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van dit beleid zijn:

- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Krimpenerwaard 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 het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, incidentregistraties 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.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B en W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directie stelt tactisch informatiebeveiligingsbeleid en jaarlijks het informatiebeveiligingsplan vast.
- De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de informatie, informatiesystemen en procesautomatiseringssystemen die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten worden opgenomen in beveiligings- of auditplannen.
- De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teammanagers zijn verantwoordelijk voor de borging van informatiebeveiliging binnen de processen waarvoor zij verantwoordelijk zijn.
- De teammanagers zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.



- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Teammanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.

De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- Informatiebeveiliging maakt deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
 - dit informatiebeveiligingsbeleid;
 - de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
 - andere audit resultaten;
 - het dreigingsbeeld gemeenten van de IBD;
 - de door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een DPIA.
- Om uitvoering te kunnen geven aan dit strategisch beleid en het informatiebeveiligingsplan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.



3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement, de eerste lijn, verantwoordelijk voor de eigen processen. De tweede lijn (CISO, Privacy Officer, Security Officer) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA-coördinator.

3.1 Aansturing: directieteam

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager. De directie zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

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

3.2 Uitvoering: teammanagers

Informatiebeveiliging valt onder de verantwoordelijkheden van de teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van de teammanagers 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, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO bij nieuwe of gewijzigde processen.
- Het (laten) uitvoeren van risicoanalyses voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

3.3 Controle en verantwoording

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



3.3.1 ENSIA

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

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.

Middels deze verantwoording worden het bestuur van de gemeente Krimpenerwaard en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Krimpenerwaard informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.