Rekenkamer Heusden

Is de gemeente Heusden digitaal veilig? Een onderzoek naar de lokale aanpak

15 september 2025

Inhoud

1. Voorwoord

Hierbij treft u de rapportage aan van het onderzoek van de rekenkamer naar digitale veiligheid in de gemeente Heusden.

Mede naar aanleiding van onderzoeksuggesties van raadsfracties, heeft de rekenkamer afgelopen voorjaar besloten dit thema onder de loep te nemen. Het doel was te onderzoeken of de voorwaarden voor digitale veiligheid goed zijn nagekomen en getoetst.
Dit onderzoek is door de rekenkamer zelf uitgevoerd. Rekenkamerlid Frank Bongers was daarbij de kartrekker/onderzoeker.

De hoofdconclusie van het onderzoek is dat de gemeente Heusden in de afgelopen jaren een solide basis heeft gelegd voor digitale veiligheid met een compleet en actueel beleidskader en de benodigde organisatorische structuur. Dit heeft geleid tot aantoonbare verbeteringen en een beheersbaar incidentenniveau.
Om de toekomstbestendigheid en doeltreffendheid van dit beleid verder te waarborgen doet de rekenkamer enkele aanbevelingen.

De rekenkamer is verheugd te constateren dat het college instemt met de aanbevelingen en dankt de ambtelijke gesprekspartners voor hun actieve medewerking aan ons onderzoek.

Frits van Vugt, voorzitter
Frank Bongers, lid
Kees Nauta, lid
Vince Janssen, secretaris

2. Samenvatting

Achtergrond en aanpak van het onderzoek

De gemeente Heusden digitaliseert steeds verder, net als andere gemeenten. Dit brengt grote voordelen met zich mee, maar ook risico's. Grote hoeveelheden, vaak privacygevoelige, gegevens worden opgeslagen en uitgewisseld. Dit maakt de gemeente een potentieel doelwit voor cyberaanvallen. Een recent voorbeeld laat de urgentie hiervan zien: in 2023-2024 werden maar liefst 150 gemeenten aangevallen met ransomware, gijzelsoftware die systemen versleutelt en toegang blokkeert. Hoewel Heusden gelukkig niet tot deze groep behoorde, kunnen zulke aanvallen (wanneer ze succes hebben) enorme schade toebrengen en hoge kosten met zich meebrengen.

Mede naar aanleiding van onderzoeksuggesties van raadsfracties, heeft de rekenkamer besloten de digitale veiligheid van de gemeente Heusden onder de loep te nemen. Het doel is te onderzoeken of de voorwaarden voor digitale veiligheid goed zijn nagekomen en getoetst.

Digitale veiligheid is een breed en complex onderwerp, dat varieert van identiteitsbeheer tot netwerkbeveiliging en risicomanagement. Om het onderzoek behapbaar te houden, heeft de rekenkamer specifieke keuzes gemaakt:

- **Geen 'live' testen:** De rekenkamer zal niet zelf de digitale veiligheid testen door bijvoorbeeld systemen of netwerken te (laten) hacken. In plaats daarvan ligt de focus op de aanwezigheid van de juiste voorwaarden voor een doeltreffend digitaal veiligheidsbeleid.
- **Volgen van gangbare praktijken:** Het onderzoek kijkt of de gemeente zich baseert op breed aanvaarde richtlijnen en afspraken voor digitale veiligheid. Het idee hierachter is: als de gemeente de best practices volgt, is de kans op incidenten kleiner. En mocht er toch iets misgaan, dan kan de gemeente adequaat handelen (incident response), een aspect dat steeds meer aandacht krijgt. Het gaat er niet om elk toekomstig digitaal veiligheidsprobleem te voorkomen, maar wel om snel te kunnen reageren.
- **Geen focus op specifieke applicaties of dagelijkse handelingen:** Dit onderzoek richt zich niet op zaken als videobellen of het updaten van software en wachtwoorden, aangezien dit type onderzoek al eerder in een rekenkamerbrief (2021) aan de orde is gekomen. Wel wordt kort ingegaan op de opvolging van aanbevelingen uit die eerdere brief.

Kortom, de rekenkamer wil een beeld krijgen van de basis en de paraatheid van de digitale veiligheid van de gemeente Heusden, zodat zij – en haar inwoners – beschermd blijven in een digitale wereld. Hierna tonen we onze hoofdconclusie en aanbevelingen.

Onze hoofdconclusie van het onderzoek

De gemeente Heusden heeft in de afgelopen jaren een solide basis gelegd voor digitale veiligheid met een compleet en actueel beleidskader en de benodigde organisatorische structuur. Dit heeft geleid tot aantoonbare verbeteringen en een beheersbaar incidentenniveau. Om de toekomstbestendigheid en doeltreffendheid van dit beleid verder te waarborgen, is het cruciaal dat de gemeente de beleidskaders operationeel volledig uitwerkt en vastlegt, de bewustwording en het gedrag van medewerkers traint en achterstanden in risicomanagement proactief wegwerkt, terwijl zij voortdurend alert blijft op nieuwe dreigingen en noodzakelijke testen uitvoert.

Onze aanbevelingen

Er zijn dus verbeterpunten om digitale risico's te blijven beheersen en de gemeente op het vlak van digitale veiligheid toekomstbestendig te maken:

1. **Versterk en complementeer de interne uitwerking van de beleidskaders voor digitale veiligheid**. Hoewel de beleidskaders compleet en actueel zijn, ontbreekt het nog aan de volledige operationele uitwerking en vastlegging. Zorg dat alle toekomstige evaluaties, inclusief die van het beleid informatiebeveiliging en privacy, worden vastgelegd in een afzonderlijk evaluatieverslag. Dit zorgt voor aantoonbaarheid, consistentie en overdraagbaarheid van kennis.
2. **Intensiveer training voor en bewustwording van digitale veiligheid.** Blijf investeren in het vergroten en onderhouden van kennis, houding en gedrag op het gebied van digitale veiligheid voor *alle* medewerkers en dat bij voorkeur met een verplicht programma. Dit is meer dan deelname aan *Sir Askalot* en de training van nieuwe medewerkers door het team Informatie & Privacy (team I&P). Overweeg gesimuleerde aanvallen (bijvoorbeeld een phishing-mail of pen-test) om de bewustwording en weerbaarheid van medewerkers (in het echt) te testen en te vergroten.
3. **Elimineer achterstanden bij het risicobeheer.** Er dreigt achterstand bij het waarborgen van digitale veiligheid bij nieuwe processen en applicaties, met name door de achterstand in *Data Protection Impact Assessments (DPIA's)* en het opschonen van oude data (verouderde e-mails en bestanden). Geef prioriteit aan het uitvoeren van alle openstaande DPIA's voor nieuwe en bestaande digitale processen en applicaties. Start of versnel opruimacties van oude mailberichten en documenten om risico's te mitigeren en compliance te verbeteren.
4. **Blijf proactief innoveren en controleren.** Het bewaken en bevorderen van digitale veiligheid is een continu proces dat nooit af is. Het is essentieel om alert te blijven op nieuwe risico's en technologieën. Integreer een proces voor de regelmatige herijking en aanpassing van het digitale veiligheidsbeleid op basis van nieuwe technologische ontwikkelingen, zoals artificiële intelligentie.

3. Inleiding

3.1 Aanleiding voor het onderzoek

De gemeente Heusden digitaliseert haar bedrijfsvoering en dienstverlening – net als andere gemeenten – steeds verder. Het opslaan en uitwisselen van grote en soms privacygevoelige gegevens vereist dat de gemeente zich wapent tegen eventuele cyberaanvallen. In de periode 2023-2024 waren er bijvoorbeeld 150 gemeenten aangevallen met ransomware.[1] Dat is gijzelsoftware die gebruikers gijzelt door hun bestanden te versleutelen en/of de toegang tot hun systeem te verhinderen. Cybercriminelen gebruiken deze software om slachtoffers af te persen. De gemeente Heusden behoorde (gelukkig) niet tot deze groep van 150 gemeenten die met deze software (bijna altijd zonder succes) werden aangevallen. Deze en andere aanvallen kennen (wanneer ze succes hebben) een hoog afbreukrisico en kunnen gepaard gaan met hoge kosten. De rekenkamer heeft mede naar aanleiding van een consultatie bij de raadsfracties beslist een onderzoek te doen naar de digitale veiligheid van de gemeente Heusden. In dit onderzoek wil de rekenkamer nagaan of de voorwaarden die voor digitale veiligheid nagekomen en getoetst worden. Het gaat dus om een wat kleiner onderzoek.

3.2 Afbakening van het onderzoek

Digitale veiligheid staat niet op zichzelf. Het is onderdeel van het breder veiligheidsbeleid dat ook fysieke en sociale veiligheid omvat. Digitale veiligheid kent ook weer verschillende onderdelen. Het omvat een breed scala aan maatregelen en praktijken om systemen, netwerken, apparaten en data te beschermen tegen dreigingen (zowel extern als intern). Er kan hierbij gedacht worden aan bijvoorbeeld identiteits- en toegangsbeheer, gegevens- en netwerkbeveiliging, beveiligingsbewustzijn en risicobeheer.

Vanwege de breedte van het onderwerp digitale veiligheid is een afbakening gewenst. De rekenkamer richt zich in dit onderzoek op de aanwezigheid van de voorwaarden voor een (doeltreffend) digitaal veiligheidsbeleid. Zij gaat de digitale veiligheid niet zelf vaststellen aan de hand van bijvoorbeeld een echte test van de organisatie, systemen of netwerken. Zij gaat wel na of de gemeente zich baseert op gangbare praktijken en afspraken ter bevordering van digitale veiligheid. Wanneer de gemeente zich baseert op breed aanvaarde richtlijnen voor de bevordering van digitale veiligheid is de kans op een incident ook kleiner; en dat wanneer er zich toch een incident voordoet de gemeente adequaat kan handelen. Vooral dit laatste (‘incident response’) krijgt steeds meer aandacht. Niet elk toekomstig digitaal veiligheidsprobleem is te voorkomen, maar het is wel mogelijk om de organisatie zodanig in te richten dat er snel gehandeld wordt bij incidenten.

Een andere afbakening is dat het onderzoek zich niet richt op specifieke applicaties of handelingen als videobellen of het updaten en actualiseren van software en wachtwoorden. Dit type onderzoek is eerder in een brief van de rekenkamer aan de orde gekomen.[2] Wel wordt kort aangeven welk vervolg de gemeente aan deze rekenkamerbrief heeft gegeven.

[1] VNG/Informatiebeveiligingsdienst (2025), Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2025 → 2026, Den Haag.
[2] Rekenkamer Heusden (2021), Digitale veiligheid in tijden van corona, Rekenkamerbrief.

3.3 Doel en onderzoeksvragen

De doelstelling van dit onderzoek is na gaan hoe de gemeente Heusden haar digitale veiligheid waarborgt en of deze borging actueel, volledig en toekomstbestendig is. In dit onderzoek beantwoorden we de volgende tien onderzoeksvragen:

1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente Heusden voor de borging van digitale veiligheid?
2. Hoe heeft de gemeente Heusden opvolging gegeven aan de bevindingen en adviezen uit de rekenkamerbrief “Digitale veiligheid in tijden van corona”?
3. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van de Baseline Informatiebeveiliging Overheid (BIO)?
4. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?
5. Hoe worden medewerkers betrokken bij en getraind in het borgen van digitale veiligheid?
6. Hoe geeft de gemeente Heusden invulling aan het testbeleid en de auditing op digitale veiligheid?
7. Op welke wijze worden de informatie- en communicatietechnologie voorzieningen (ICT-voorzieningen) (waaronder de infrastructuur, de wifi, de volledige werkplek, de website en digitale dienstverlening) van de gemeente Heusden getest op digitale veiligheid, met welke frequentie en met welke resultaten?
8. Welke mogelijke risico’s zijn te onderkennen in de huidige wijze waarop digitale veiligheid is ingericht en functioneert?
9. Hoe ziet de gemeente erop toe dat digitaal veiligheidsbeleid van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven?
10. Welke beveiligingsincidenten heeft de gemeente Heusden in de afgelopen twee jaren ondervonden en hoe zijn deze afgewikkeld? Is de ‘incident response’ van de gemeente Heusden op orde?

Box 1: Beschrijving van de Baseline Informatiebeveiliging Overheid (BIO) [3]

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Voorheen had elke overheidslaag een eigen baseline. Nu is er met gezamenlijke inspanning één BIO voor de gehele overheid.

De BIO onderscheidt drie Basisbeveiligingsniveaus (BBN's), waarbij het benodigde beveiligingsniveau wordt bepaald op basis van de gevoeligheid van de informatie en de mogelijke impact bij een incident:

- BBN1: De nadruk ligt op wat minimaal verwacht mag worden van alle overheidssystemen.
- BBN2: Richt zich op de bescherming van de meest voorkomende categorieën informatie, volgens het principe van "goed huisvaderschap": toont deze beveiliging de betrouwbare overheid?
- BBN3: Voor de meest gevoelige informatie, waar zwaardere beveiligingsmaatregelen nodig zijn.

De BIO geeft een aantal op te volgen richtlijnen ten aanzien van bijvoorbeeld aansturing door de directie van de informatiebeveiliging, interne organisatie, mobiele apparatuur en telewerken en personeel.[4]

3.4 Aanpak van het onderzoek

De aanpak bestaat van dit onderzoek bestaat uit de volgende activiteiten, namelijk:

[3] De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Zie [Baseline Informatiebeveiliging Overheid Cybersecurity - Digitale Overheid].
[4] Zie ook [bio-versie-104zv_def.pdf].

1. Verkennend gesprek met de Chief Information Security Officer (CISO) en de Clustermanager I&A (Informatie & Automatisering) van de gemeente Heusden met oog op aanscherpen van de onderzoeksaanpak.[5]
2. Startgesprek met portefeuillehouder (burgemeester) en de CISO en de manager I&A van de gemeente Heusden.[6]
3. Verzameling en analyse van relevante landelijke en lokale documenten over digitale veiligheid.
4. Afzonderlijke interviews met de CISO, clustermanager I&A, de Privacy Officer (PO) en een vertegenwoordiging van medewerkers van de gemeente Heusden over het digitale veiligheidsbeleid van de gemeente Heusden.[7]
5. Toetsing resultaten aan normenkader (zie Bijlage 2; tegelijk beantwoording van de onderzoeksvragen);
6. Concept- en eindrapportage (inclusief ambtelijke en bestuurlijke wederhoor).

[5] Dit gesprek vond op 20 maart 2025 plaats.
[6] Dit gesprek vond op 23 april 2025 plaats op basis van een aangescherpte onderzoeksaanpak.
[7] De CISO en clustermanager I&A hebben bij aanvang de onderzoeksvragen (zie paragraaf 0) in een aparte notitie beantwoord. Deze notitie is te beschouwen als een beperkte zelfevaluatie en gaf de rekenkamer (extra) aanknopingspunten voor de documentenanalyse en de interviews (onder meer om de antwoorden te verdiepen en te toetsen).

4. Nota van bevindingen

4.1 Inleiding

In dit hoofdstuk presenteren we de resultaten van het onderzoek verdeeld over zes paragrafen. Achtereenvolgens komen aan de orde: Beleidskaders voor digitale veiligheid (en hun uitwerking), de betrokkenheid van medewerkers bij digitale veiligheid, het testbeleid (en resultaten), risico's en incidenten, de vorige Rekenkamerbrief digitale veiligheid en de toekomstvastheid van het digitaal veiligheidsbeleid.

4.2 Beleidskaders en organisatie

In deze paragraaf gaan we na welke beleidskaders de gemeente Heusden hanteert voor het bevorderen en bewaken van digitale veiligheid en in welke mate deze kader vertaald zijn naar de werkvloer (onderzoeksvragen 1, 3 en 4). Dit in onze veronderstelling dat het hanteren van complete en actuele kaders bijdraagt aan digitale veiligheid.

4.2.1 Integraal veiligheidsplan

In het lopend **Integraal Veiligheidsplan gemeente Heusden 2023-2026**[8] is digitale veiligheid één van de vier strategische thema's. De uitgevoerde activiteiten in 2023-2024 en daarna betreffen:

- Verdere implementatie/op peil houden integrale informatiebeveiligingsorganisatie.
- Investeren in houding en gedrag medewerkers door onder meer voorlichting/communicatie, regelmatige controles/tests.
- Uitwerken continuïteitsplan (koppelen aan regionaal crisisplan/crisisbeheersing)
- Implementatie BIO (Baseline Informatiebeveiliging Overheid) (Zie Box 1).
- ENSIA (Eenduidige Normatiek Single Information Audit) (Zie Box 2).

Box 2: Beschrijving van de Eenduidige Normatiek Single Information (ENSIA)[9]

ENSIA is ontstaan vanuit een gezamenlijk initiatief van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Infrastructuur en Milieu, Sociale Zaken en Werkgelegenheid en de Vereniging van Nederlandse Gemeenten (VNG). Het doel van ENSIA is om tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te komen, gebaseerd op de BIO (Zie Box 1).

ENSIA is per 1 juli 2017 ingevoerd en inmiddels laten zeven informatiestelsels hun verantwoordingssystematiek via ENSIA verlopen:

- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)

Uitgangspunt voor het ENSIA-verantwoordingsstelsel is het horizontale verantwoordingsproces. In dit proces verantwoordt (voor de gemeente Heusden) het college zich over informatieveiligheid aan de raad. Dit wordt horizontaal toezicht genoemd. De horizontale verantwoording vormt de basis voor het verticale verantwoordingsproces richting de (centrale) toezichthouders van de genoemde informatiestelsels.

[8] Zie [Document Heusden - BIJL Integraal Veiligheidsplan gemeente Heusden 2023-2026 20221220 - iBabs Publieksportaal].
[9] Zie [ENSIA Cybersecurity - Digitale Overheid].

ENSIA is dus een verantwoordingsinstrument over informatiebeveiliging en datakwaliteit. Zij ondersteunt gemeenten bij het verwerven van inzicht in de risico's op het vlak van informatiebeveiliging en helpt gemeenten om maatregelen te nemen.[10]

4.2.2 Beleid informatiebeveiliging en privacy

Het belangrijkste lopend beleidskader voor digitale veiligheid betreft **Beleid informatiebeveiliging en privacy 2024-2028 Gemeente Heusden**.[11] Dit kader vermeldt de geldende principes en uitgangspunten voor de gemeente Heusden. Als leidende principes gelden: (1) gemeente stelt de klant centraal; (2) de gemeente gaat de dialoog aan en werkt samen; en (3) de gemeente spreekt aan en neemt verantwoordelijkheid. In de volgende box staan meer gedetailleerde uitgangspunten voor dit beleid.

Box 3: Gemeentelijke uitgangspunten informatiebeveiliging en privacy

- Met haar informatiebeveiliging wil de gemeente ervoor zorgen dat zij haar maatschappelijke opgaves realiseert, rekening houdt met geldende wet- en regelgeving.
- Naleving van de BIO en de AVG[12] (en eventuele toekomstige relevante wet- en regelgeving) vormt de basis voor haar informatiebeveiliging en rechtmatige verwerking van (persoons)gegevens.
- Deze regelgeving is tevens leidend en bepalend voor de leveranciers en andere partners met wie wordt samengewerkt. Informatiebeveiliging en privacy worden ook meegenomen bij het opzetten en uitvoeren van (keten)samenwerking. Er worden afspraken gemaakt op het gebied van Informatiebeveiliging en privacy en op de `naleving wordt toegezien.
- Het inrichten van de informatievoorziening volgens dit beleid in opzet, bestaan en werking, geeft afdoende garantie voor haar informatiebeveiliging en het rechtmatig verwerken van persoonsgegevens.
- Het beveiligingsniveau is in lagen uitbreidbaar. Dit betekent dat de basis uitgaat van de BIO en de AVG. Daar waar nodig of vereist, worden extra maatregelen getroffen boven op dit basisniveau. Een uitgevoerde risicoanalyse kan hiertoe aanleiding geven. Daarnaast kan wet- en regelgeving hier de gemeente toe verplichten.
- Dit beleid en deze beleidsregels worden uitgewerkt in een tactisch plan zodat de naleving van het beleid op tactisch en operationeel niveau is opgezet en wordt nageleefd.
- Bij de start van projecten, het inrichten processen en het inkopen of uitbesteden van systemen wordt een risicoanalyse vroegtijdig uitgevoerd en expliciet een besluit genomen door de risico-eigenaar (lijn manager) op de beheersing van de gevonden risico's en de opvolging van het advies.
- Het primaire uitgangspunt voor dit beleid is risicomanagement. De gemeente hanteert voor informatiebeveiliging de risicomanagementsystematiek volgens de BIO (een afgeleide van de NEN-ISO 27001 en 27002-normen). Hiervoor brengt zij continu risico's in beeld, treft waar nodig passende beheersmaatregelen en monitort zij of de beheersmaatregelen over de tijd heen nog steeds effectief en efficiënt werken.
- Informatie wordt geclassificeerd om te bepalen welke beveiligingsmaatregelen nodig zijn. Hierbij is de aard van de informatie in de processen leidend. Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Op basis van een classificatie wordt bepaald hoe deze informatie behandeld dient te worden.
- Het principe van 'Security and privacy by design and default'[13] staat centraal. Dit betekent dat optimale privacy en informatiebeveiliging wordt betracht en dat dit tevens wordt meegenomen bij de ontwikkeling en inrichting van informatiesystemen, processen en diensten.
- Veilig omgaan met informatie is een verantwoordelijkheid van alle medewerkers in de hele organisatie. Verantwoord en bewust gedrag is essentieel. Structureel en planmatig wordt gewerkt aan het bewustzijn. Ook hierbij gaat de gemeente uit van haar Heusdense principes.
- Via de P&C-cyclus wordt horizontaal verantwoording afgelegd door het college van B&W aan de gemeenteraad. Er wordt gewerkt conform de plan-do-check-act verbetercyclus. De verticale verantwoording aan de verantwoordelijke stelselhouders leunt op de horizontale verantwoording

[10] Zie [Zie [ENSIA | VNG].
[11] Zie [Beleid informatiebeveiliging en privacy 2024-2028 Gemeente Heusden | Lokale wet- en regelgeving].
[12] Algemene Verordening Gegevensbescherming. Zie [De AVG in het kort | Autoriteit Persoonsgegevens]
[13] Zie voor een uitleg van deze begrippen [Verantwoordingsplicht | Autoriteit Persoonsgegevens]

en vindt plaats door middel van ENSIA. Voor implementatie en uitwerking van voorliggend beleid, wordt een doorvertaling gemaakt van dit beleid in een tactisch plan voor informatiebeveiliging en privacy. Dat plan wordt waar nodig vertaald in vakspecifieke procedures en/of werkwijzen. Dit gebeurt in ieder geval voor het waarborgen van de eisen die voortvloeien uit de verschillende stelsels, zoals Suwinet, DigiD en de basisregistraties (waaronder BRP, BAG, BGT, BRO[14]).

- Vakspecifiek(e) procedures, werkinstructies en dergelijke ten aanzien van Informatiebeveiliging en privacy worden op het laagst mogelijke niveau vastgesteld door de verantwoordelijke. Indien het alleen betrekking heeft op één team, dan kan de lijnmanager dit op het laagste niveau vaststellen.
- De gemeente gebruikt een beveiligingsmodel[15] waar de digitale identiteit als ook het digitale apparaat altijd eerst expliciet geverifieerd worden voordat het toegang krijgt tot haar data. Hierbij worden niet meer rechten verstrekt dan noodzakelijk (need-to-know) en gebruik gemaakt van tweefactorauthenticatie. Aansluitend wordt onze gehele IT-infrastructuur en haar data (ongeacht waar deze staat) passend beveiligd. Er vindt uitgebreide monitoring en logging[16] plaats om digitale dreigingen vroegtijdig te signaleren en te herkennen.
- De gemeente gaat er vanuit dat er een reële kans is te worden getroffen door een digitale dreiging. Zij zorgt ervoor hierop voorbereid te zijn om zo de impact te minimaliseren en snel te kunnen herstellen van een incident. Hiermee zo de afgesproken bedrijfscontinuïteit te garanderen.

Deze principes en uitgangspunten (Box 3) vormen de fundering voor het gemeentelijk beleid gericht op digitale veiligheid. De belangrijkste (landelijke) kaders vormen de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO). Deze kaders zijn van toepassing op alle overige (deel)beveiligingsplannen die bijvoorbeeld opgesteld worden voor de basisregistraties BRP, BGT, BRO en de BAG, maar ook DigiD, Suwinet, Paspoorten en ID-bewijzen.

De betreffende beveiligingsplannen staan echter op zichzelf en dat blijft volgens de gemeente zo omdat daarin de specifieke maatregelen, procedures, regelingen en bijlagen in staan.

In onze interviews kwam naar voren dat de gemeentelijke organisatie op dit moment een inhaalslag maakt om (de kennis over en ervaring met) digitale veiligheid verder op schrift te stellen. Het college benoemt in het Beleid informatiebeveiliging en privacy 2024-2028 Gemeente Heusden de uitgangspunten die vertaald worden naar een tactisch plan Informatiebeveiliging en privacy dat door het MT zal worden vastgesteld. Dit tactisch plan bevat onder meer operationele plannen, acties en procedures. De uitwerking en vaststelling moeten dus nog gebeuren.

Dit beeld over de inhaalslag blijkt ook uit het laatste jaarverslag van de Functionaris Gegevensbescherming. Op het vlak van gegevensbescherming zijn de kaders vastgelegd en bekend, maar de borging is soms nog onvoldoende bijvoorbeeld vanwege het ontbreken van werkinstructies.[17]

4.2.3 Functionarissen digitale veiligheid

Naast deze principes en uitgangspunten kent de gemeente Heusden in de interne organisatie een aantal functionarissen dat het beleid en de maatregelen voor het bevorderen van digitale veiligheid ontwikkelt, uitvoert, monitort en (bij)stuurt, zoals:

- College van B&W (Burgemeester als portefeuillehouder)
- Managementteam (MT) (Gemeentesecretaris als portefeuillehouder)

[14] Basisregistratie Personen (BRP), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO).
[15] Zie [Factsheet Bereid u voor op Zero Trust | Factsheet | Nationaal Cyber Security Centrum].
[16] Logging betreft het automatisch bijhouden van gegevens over bepaalde gebeurtenissen (bijvoorbeeld het aantal website bezoekers).
[17] [Jaarverslag 2024 Functionaris Gegevensbescherming Gemeente Heusden], p. 7.

- Chief Information Security Officer (CISO)[18]
- Privacy Officer (PO)[19]
- Functionaris Gegevensbescherming (FG)[20]
- Clustermanager Informatisering en Automatisering (I&A)

Ook is er een iTeam[21] actief dat momenteel een iVisie uitwerkt voor de gemeente. Het primaire doel van de iVisie is het creëren van een helder en overkoepelend kader voor het informatiebeheer binnen de gemeente Heusden. Deze visie (waarin veiligheid ook aan de orde komt) is onder de naam i-MogelijkMaken vastgesteld door het MT.[22]

Daarnaast hebben alle andere medewerkers van de gemeente een verantwoordelijkheid om in hun dagelijks werk digitale veiligheid na te streven (zie ook paragraaf 4.3).

Het beleid informatiebeveiliging en privacy 2024-2028 wordt minimaal één keer per jaar geëvalueerd onder leiding van de CISO en PO. De evaluatie vindt plaats middels een presentatie in het MT waarin het voorgaande jaar wordt geëvalueerd en waar een plan voor het volgend jaar wordt gepresenteerd en vastgesteld. De verslaglegging van de evaluatie geschiedt via de (intern openbare) MT notulen.

4.3 Betrokkenheid van de bredere organisatie

Beleidskaders en (technische) systemen kunnen op orde zijn. Digitale veiligheid is en blijft uiteindelijk ook mensenwerk. Wanneer lijnmanagers onvoldoende sturen op digitale veiligheid of medewerkers de interne richtlijnen onvoldoende kennen en gebruiken blijven er risico's ten aanzien van digitale veiligheid bestaan. In deze paragraaf gaan we na hoe de bredere organisatie (dus buiten de "IT-kolom") betrokken wordt bij digitale veiligheid (onderzoeksvraag 5).

Het is mogelijk om digitale veiligheid technisch goed te organiseren, maar het vergt kennis, vaardigheden en medewerking van *alle* medewerkers. Uit onze gesprekken blijkt dat medewerkers zich bewust zijn van de rol die zij zelf spelen bij digitale veiligheid. Uit deze gesprekken blijkt verder dat over het algemeen de aandacht voor digitale veiligheid binnen de gemeentelijke organisatie goed is. De verantwoordelijke functionarissen voelen zich (bestuurlijk) gesteund door het college (in bijzonder door de burgemeester die dit dossier in haar portefeuille heeft) en het managementteam. De bestuurders en managers zijn geen specialist in dit onderwerp (wat ook niet nodig is volgens ons). Zij erkennen wel het belang van digitale veiligheid, zijn makkelijk benaderbaar over dit onderwerp en ondersteunen het ontwikkelen, implementeren en handhaven van kaders waar dat nodig is.

In de afgelopen drie jaar heeft het college (en de portefeuillehouder digitale veiligheid in het bijzonder) de raad op verschillende momenten geïnformeerd over dit onderwerp. Op 4 april 2023 is in een Raadsinformatiebrief teruggekoppeld over de uitvoering van het Integraal Veiligheidsplaan gemeente Heusden 2023-2026.[23] In dit plan is digitale veiligheid één van de vier strategische thema's.

[18] De CISO is verantwoordelijk voor de informatiebeveiliging binnen de gemeente. Dit omvat het ontwikkelen, implementeren en beheren van het informatiebeveiligingsbeleid, het identificeren en mitigeren van beveiligingsrisico's en het waarborgen van de naleving van relevante wet- en regelgeving,

[19] De PO is verantwoordelijk voor het waarborgen van de privacy van persoonsgegevens de gemeente. De PO ontwikkelt en implementeert privacybeleid, adviseert medewerkers over gegevensbescherming, en zorgt voor bewustwording rondom privacy. De PO monitort de verwerking van persoonsgegevens, beoordelen privacyrisico's en handelt datalekken af.

[20] De FG is een onafhankelijke expert binnen de gemeente die toezicht houdt op de naleving van privacywetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). De FG adviseert, informeert en controleert de gemeente over hoe persoonsgegevens worden verwerkt en beschermd.

[21] Het iTeam is een multidisciplinaire samenwerking rondom informatiebeheer met betrokkenen vanuit de clusters documentaire informatievoorziening (DIV), informatie & automatisering (I&A), kwaliteitscontrol (KC), CISO en de Privacy Officer (PO).

[22] I-MogelijkMaken. Informatiebeheer Gemeente Heusden.

[23] Zie [Document Heusden - BIJL Integraal Veiligheidsplan gemeente Heusden 2023-2026 20221220 - iBabs Publieksportaal]

De gemeente Heusden investeert in het betrekken van medewerkers bij en het trainen van medewerkers in het borgen van digitale veiligheid. Dit wordt bevestigd in een interview met vijf gemeentelijke medewerkers. Het werken aan bewustwording in de organisatie is ook een AVG- en BIO-vereiste. Dit gebeurt aan de hand van het nanolearning bewustwordingsprogramma *Bewust in Control*.[24] *Sir Askalot* stelt wekelijks via e-mail korte vragen over deze onderwerpen om deze kennis actief te houden. Ongeveer de helft van de gemeentelijke medewerkers doet mee aan *Sir Askalot*.[25] De geïnterviewde gemeentelijke medewerkers ervaren *Sir Askelot* (voor zover zij dat gebruiken) als een laagdrempelig en effectief middel om digitale veiligheid onder de aandacht te brengen en te houden. Tegelijk bestaat het risico dat dit programma na verloop van tijd wat sleets wordt.

Ook worden er elke week berichten geplaatst op het intranet met actuele thema's rond informatiebeveiliging en privacy. Binnen de 'Heusdense School' worden jaarlijks sessies georganiseerd, zoals een workshop 'hacken' die vorig jaar is gegeven aan de I&A-afdeling. Verdiepende kennis en vaardigheden omtrent digitale veiligheid is vooral nodig voor medewerkers die bijvoorbeeld met privacygevoelige gegevens werken. Voor hen bestaat altijd de mogelijkheid voor extra scholing.

Alle medewerkers worden bij indiensttreding geïnformeerd over het belang van digitale veiligheid. Er bestaat een maandelijkse introductietraining informatiebeveiliging & privacy voor nieuwe medewerkers door het team Informatie & Privacy (team I&P).[26] Dit als onderdeel van een breder introductieprogramma. Hoewel deelname niet verplicht is, worden nieuwe medewerkers – indien nodig herhaaldelijk – uitgenodigd deel te nemen. Daarbij constateren betrokkenen dat vooral jongere medewerkers steeds vaker relevante kennis en vaardigheden meebrengen die voor digitale veiligheid relevant is (ze zijn er meer mee opgegroeid). Dit als onderdeel van de bredere observatie dat jongeren digitaal vaardiger zijn dan ouderen.

Dit alles (bestuurlijke aandacht, training, etc.) helpt aan structurele bewustwording over digitale veiligheid en versterkt het menselijk aspect bij digitale veiligheid. Het beeld is dat de medewerkers in vergelijking met enkele jaren geleden digitaal vaardiger zijn (maar er ontbreken cijfers om dat te onderbouwen; de rekenkamer heeft dit ook niet onderzocht met bijvoorbeeld een interne test of vragenlijst). Uit ons gesprek met vijf gemeentelijke medewerkers blijkt ook dat er in de organisatie een (groeiende) cultuur ontstaat over het elkaar wijzen op onveilig digitaal gedrag en dat bij twijfel medewerkers elkaar helpen (of ondersteuning zoeken bij I&A). Dit alles onder het mom van het gebruik van het gezonde verstand. Ook groeit het aantal (technische) maatregelen gericht op digitale veiligheid. Sommige geïnterviewde medewerkers wijzen erop dat het inloggen steeds meer tijd kost, maar er is ook wel begrip voor dit soort procedures om de veiligheid te borgen. Deze medewerkers constateren ook dat de crisiscommunicatie bij incidenten niet goed loopt. Dat bijvoorbeeld een Whatsapp bericht naar alle medewerkers wordt gestuurd zodra er geen mogelijkheid is om in te loggen. Het heeft geen zin een storing op HEIN (het gemeentelijke intranet) te plaatsen als er niet ingelogd kan worden.

4.4 Testen, audits en resultaten

De vraag of de gemeente beleidsmatig, technisch en organisatorisch voldoet aan de eisen die digitale veiligheid stelt, wordt via verschillende kanalen regelmatig onderzocht. Dit helpt om de organisatie

[24] Nanolearning richt zich op het snel en effectief beschikbaar maken van kennis en vaardigheden aan de hand van het frequent aanbieden van kleine brokjes informatie voor het behalen van een bepaald (leer)resultaat (in dit geval dus over informatiebeveiliging).
[25] De deelname aan Sir Askalot steeg tussen juni 2024 en juni 2025 van 43% naar 52% (bron: Rapportage bewustwordingsprogramma Informatiebeveiliging & Privacy (Sir Askalot) (14 juni 2024 & 2 juni 2025). Dit is volgens ons een indicatie dat medewerkers meer inspanning tonen zich te trainen in vaardigheden voor digitale veiligheid.
[26] Zie [Informatiebeveiliging en privacy | Jaarstukken 2024].

fit te houden en aan te passen waar dat nodig is. Deze paragraaf richt zich op de vraag welke activiteiten de gemeente ontplooit om de kwaliteit van de organisatie en systemen op het vlak van digitale veiligheid te monitoren (onderzoeksvragen 6 en 7).

4.4.1 Interne audits

In 2024 heeft de gemeente interne ENSIA-audits uitgevoerd van de BRP, BAG, BGT, BRO, DigiD en Suwinet.[27] Dit zijn zes van de zeven informatiestelsels die hun verantwoordingssystematiek via ENSIA laten verlopen (zie Box 2). Uit de collegevoorstellen en -verklaringen blijkt dat de gemeente Heusden goed voldoet aan ENSIA en de beveiligingsrichtlijnen voor DigiD. De BRP scoort goed op de inrichting, de werking en de beveiliging. De BAG, BGT en BRO scoren ook goed en vergen geen directe verbetermaatregelen. Wel is blijvende aandacht nodig voor de kwaliteitseisen. De rekenkamer heeft op 17 juni 2025 inzage gehad in twee DigiD-audits (2022 en 2024) voor de aanvraag van leerlingenvervoer in de gemeente Heusden[28] dat onderdeel is van het zorgportaal Heusden. Uit beide audits blijkt dat de gemeente voldoet aan alle beveiligingsrichtlijnen voor DigiD.[29]

4.4.2 Externe controles

De gemeente Heusden houdt bij het testen van digitale veiligheid rekening met het feit dat risico's steeds meer bij SaaS-leveranciers[30] liggen. Bij het gebruik van SaaS loopt de gemeente een verhoogd risico op het overnemen van gebruikersaccounts door kwaadwilligen. Dit risico is deels gerelateerd aan het feit dat SaaS wordt blootgesteld aan internet. Geografische beperkingen zijn niet gebruikelijk bij SaaS-diensten; eventuele aanvallen kunnen overal vandaan komen. Leveranciers worden door de gemeente daarom actief gemonitord via contractmanagement, onder andere op basis van het GIBIT[31]. Samen met de VNG worden grote gemeentelijke leveranciers gecontroleerd. Daarnaast worden kwetsbaarheden gemeld via Informatiebeveiligingsdienst (IBD) van de VNG.[32] op basis van de "ICT-Foto". Gemeentelijke websites worden continu bewaakt door de IBD.

Externe (ICT-)leveranciers voeren ook regelmatig controles uit op actuele thema's. In 2024 is onder meer gekeken naar het inlogproces (*conditional access*) en Intune, het systeem voor het beheer van mobiele apparaten (*mobile device management*).

Op basis van onze gesprekken met de clustermanager I&A en de CISO hebben wij het beeld dat de gemeente zich goed bewust is van de risico's van software die – in tegenstelling tot voorheen – steeds meer die als dienst wordt aangeboden (zgn. 'VerSaaSing').

[27] Zie Collegeverklaring ENSIA over informatiebeveiliging DigiD en Suwinet (29 april 2025); Collegevoorstel zelfevaluatie basisregistratie personen (BRP) (1 april 2025); ENSIA zelfevaluatie verantwoordingsrapportage BAG, BGT en BRO 2024 (1 april 2025).
[28] Zie [Aanvraag Leerlingenvervoer | Zorgportaal Heusden].
[29] Deze normen staan hier [Logius | Normenkader 3.0 voor ICT-beveiligingsassessments DigiD].
[30] SaaS betekent *Software as a Service*. Dit is software die als een online dienst wordt aangeboden. De gemeente Heusden schaft in dit geval de software niet aan, maar sluit bijvoorbeeld een contract per maand per gebruiker af. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer van de software. De gebruiker benadert de software over het internet bij de SaaS-aanbieder. Zie [Software as a Service - Wikipedia].
[31] GIBIT staat voor Gemeentelijke Inkoop bij IT Toolbox. De Toolbox bevat onder andere inkoopvoorwaarden, kwaliteitsnormen en checklisten, die gemeenten helpen bij het professionaliseren van de inkoop van ICT-diensten en –producten. Zie [GIBIT | VNG].
[32] De IBD is de sectorale *Computer Emergency Response Team* (CERT) voor alle Nederlandse gemeenten en onderdeel van de VNG. De Informatiebeveiligingsdienst (IBD) IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD draagt namens gemeenten bij aan de BIO en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. De gemeente Heusden maakt gebruik van de generieke dienstverlening van de IBD. Zie [Over de IBD - Informatiebeveiligingsdienst]

4.5 Risico's en incidenten

Ondanks de beschikbaarheid van beleidskaders en instructies, een volledig ingerichte organisatie en audits zullen er risico's blijven bestaan. Dit komt ook doordat er continu nieuwe hard- en software in gebruik worden genomen en doordat kwaadwillende steeds nieuwe manieren bedenken om digitale veiligheidsmaatregelen van hun slachtoffers te omzeilen. In deze paragraaf richten we ons op de bestaande risico's en op eventuele incidenten die zich hebben voorgedaan bij de gemeente (onderzoeksvragen 8 en 10).

4.5.1 Risico's digitale veiligheid

In de huidige aanpak van digitale veiligheid van de gemeente Heusden bestaan de volgende risico's (en vele dan deze risico's gelden voor alle gemeenten; zie ook Box 4):

- Digitale veiligheid is en blijft mensenwerk. Medewerkers en andere betrokkenen zijn zich in meer of mindere mate bewust van het belang van digitale veiligheid en kunnen fouten maken waardoor er beveiligingsincidenten ontstaan.[33] Trainings- en bewustwordingsprogramma's helpen (zie paragraaf 0), maar kunnen dit risico nooit volledig wegnemen.
- Digitale veiligheid staat meer onder druk met het groeiend gebruik van clouddiensten (voorbeeld van de eerdergenoemde 'VerSaaSing'). Dit kan leiden tot verkeerde configuratie, maar vergroot ook de zorgen over de toegang tot gegevens. Bij het gebruik van clouddiensten heeft de gemeente Heusden gegevens niet meer op een eigen server staan.
- Digitale veiligheid van de gemeente Heusden kan aangetast worden wanneer een (ICT-) leverancier aangevallen wordt door bijvoorbeeld hackers. De diensten die de gemeente dan afneemt, kunnen ook onderbroken worden.
- Digitale veiligheid vraagt in geld, kennis en capaciteit. Voor een betere beveiliging in de cloud is de gemeente Heusden overgestapt van Microsoft E3-naar E5-licenties, wat hogere kosten met zich meebrengt.[34]
- Digitale veiligheid vereist dat verwerking van persoonsgegevens voldoet aan de Algemene Verordening Gegevensbescherming (AVG). Dit betekent dat interne werkprocessen getoetst en ingericht woerden conform AVG-beginselen. Daarvoor bestaat de *Data Protection Impact Assessment* (DPIA). Vanwege de hoge werkdruk in de organisatie – ook bij de Privacy Officer – heeft de gemeente Heusden een achterstand opgelopen bij het uitvoeren en afronden van DPIA's (alleen voor veilig mailen). Er zijn momenteel wel DPIA's onder handen, maar de achterstand is moeilijk in te halen binnen de bestaande capaciteit en de prioriteit die lijnmanagers en medewerkers er aan geven.[35]
- Verder blijkt uit het laatste jaarverslag van de Functionaris Gegevensbescherming dat er geen uitgewerkt beoordelingsproces is met een managementsysteem voor het identificeren en aanpakken van risico's die samenhangen met persoonsgegevens. [36]

[33] Een concreet voorbeeld hiervan genoemd in een van de interviews is dat het voor veel medewerkers gebruikelijk is om emailberichten en documenten langer te bewaren dan nodig. Opruimacties helpen te voorkomen dat er digitale gegevens kunnen worden gelekt of gestolen.
[34] Een Microsoft 365 E3 EEA (zonder Teams) licentie kost €35,70 per gebruiker per maand. Een Microsoft 365 E5 EEA (zonder Teams) licentie kost €57,70 per gebruiker per maand. Bedragen exclusief BTW. Zie [Vergelijk Microsoft 365 Enterprise-abonnementen | Microsoft 365].
[35] Jaarverslag 2024 Functionaris Gegevensbescherming Gemeente Heusden, p. 7. Op basis van een overzicht van de Vereniging van Nederlandse Gemeenten (VNG) heeft de gemeente een selectie gemaakt van DPIA's die uiterlijk eind 2026 uitgevoerd moeten zijn. Ook is het bij de aanschaf van nieuwe applicaties voortaan standaard om vooraf een DPIA te doen (bron: interview met de PO).
[36] Jaarverslag 2024 Functionaris Gegevensbescherming Gemeente Heusden, p. 12.

Box 4: Belangrijkste bedreigingen uit het meeste recente Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten[37]

- Ransomware blijft de grootste dreiging. Criminelen gebruiken kwetsbare systemen om gevoelige data te stelen en organisaties af te persen, met aanzienlijke gevolgen zoals privacyschendingen, imagoschade en financiële verliezen.
- Incidenten bij leveranciers leiden tot verstoringen in gemeentelijke processen. Gemeenten zijn afhankelijk van externe partijen, wat de noodzaak benadrukt van duidelijke afspraken over beveiliging.
- Beperkte capaciteit, kennis en middelen bemoeilijken investeringen in digitale veiligheid.

4.5.2 Incidenten met digitale veiligheid

Uit ons bronnenonderzoek en onze gesprekken blijkt dat de gemeente – buiten de incidenten rond verwerking persoonsgegevens[38] - zeer incidenteel te maken heeft met incidenten rondom digitale veiligheid die om een snelle en effectieve reactie vragen (vanwege de grote potentiële schade die er kan optreden, bijvoorbeeld juridisch, beleidsmatig of economisch).

Het aantal van dit soort incidenten in de afgelopen jaren is op enkele vingers te tellen (wel neemt het aantal pogingen toe). Zo vond er in 2024 een hack van een mailbox plaats. Een evaluatie van deze hack heeft ertoe geleid om het bestaande incidentprotocol door te ontwikkelen naar een analogie van de GRIP-niveaus die de Veiligheidsregio's bij de opschaling van incidenten en rampen hanteren.[39] De omvang en de (potentiële) schade van een digitaal veiligheidsincident zijn dan bepalend voor de mate waarin er een interne opschaling plaatsvindt. Deze aanpak is inmiddels vastgesteld door het MT.

4.6 Rekenkamerbrief "Digitale veiligheid in tijden van corona"

Onderzoek naar de digitale veiligheid staat niet voor de eerste keer op de agenda van de rekenkamer. In de rekenkamerbrief "Digitale veiligheid in tijden van corona" [40] *noemde de vier aandachtspunten (waarvan enkele in de vorm van een aanbeveling) voor het lokaal beleid gericht op digitale veiligheid.*

In de volgende tabel staan deze aandachtspunten (en of en hoe deze door de gemeente zijn opgepakt). Dit is een antwoord op onderzoeksvraag 2.

Tabel 1. Aandachtspunten en opvolging Rekenkamerbrief Digitale Veiligheid.

Aandachtspunten	Opvolging
Raadsleden worden door de afdeling I&A of de griffie vooralsnog niet actief geïnformeerd of geadviseerd over digitale veiligheid. Met name omdat zij gebruik maken van zelf aangeschafte hardware en software en de organisatie hier dus ook geen zicht op heeft. Of deze keuzevrijheid voor raadsleden voor de toekomst nog steeds wenselijk is, is wat de rekenkamer betreft een aandachtspunt.	Met het presidium is in 2025 afgesproken dat raadsleden vrijwillig deelnemen aan het bewustwordingsprogramma "Bewust in control". Raadsleden zijn zelf verantwoordelijk voor hun informatiebeveiliging. De ipad's worden wel door de gemeente Heusden geleverd en die is ook verantwoordelijk voor de beveiliging van iBabs.

[37] VNG/Informatiebeveiligingsdienst (2025), Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2025 → 2026, Den Haag.
[38] In 2024 zijn er 21 incidenten intern gemeld waarvan er één aan de Autoriteit Persoonsgegevens is gemeld. Jaarverslag 2024 Functionaris Gegevensbescherming Gemeente Heusden, p. 11. Naarmate medewerkers zich beter bewust zijn van de bescherming van persoonsgegevens bestaat de kans dat er meer meldingen van datalekken worden gedaan dan vroeger. De incidenten betreffen doorgaans kleine zaken, bijvoorbeeld een email die aan een verkeerde persoon is verricht.
[39] GRIP staat voor Gecoördineerde Regionale Incidentbestrijdingsprocedure. Dat is een gestructureerde aanpak om ervoor te zorgen dat de juiste hulp op het juiste moment beschikbaar is. Het doel is om incidenten en rampen efficiënt en doeltreffend te bestrijden door de betrokken partijen te coördineren en de inzet van hulpverleners te optimaliseren. GRIP onderscheidt vijf niveaus. Zie ook [Instituut Fysieke Veiligheid (2022), GRIP en de flexibele toepassing ervan].
[40] Rekenkamer Heusden (2021), Digitale veiligheid in tijden van corona, Rekenkamerbrief.

	Raadsleden hebben geen toegang tot de gemeentelijke bedrijfsvoerings- en informatiesystemen en vormen daarmee dus ook geen risico voor de digitale veiligheid.
De rekenkamer raadt de gemeenteraad aan om te volgen of alle noodzakelijke aanpassingen volgend uit de nieuwe BIO gedurende 2020 daadwerkelijk gedaan zijn zodat, conform de BIO, de gemeente Heusden einde 2020 aan alle eisen voldoet. De rekenkamer stelt voor dat het college hierover rapporteert in de eerste bestuursrapportage 2021.	Er is in 2021 besloten niet via de Berap te rapporteren. De Berap gaat over financiële aangelegenheden gaat. Het college rapporteert via het jaarverslag en de begroting over de informatiebeveiliging. De implementatie van de BIO komt in de jaarlijkse collegeverklaring over de ENSIA audit aan de orde (zie ook paragraaf 4.4.1).
De rekenkamer adviseert de gemeenteraad om actief te volgen in hoeverre bij de keuze voor (meer) digitale vormen van communicatie voldoende aandacht wordt gegeven aan de adviezen van de Raad van State ten aanzien van de effecten van de digitalisering voor de rechtstatelijke verhoudingen. Dit zou kunnen als vast onderdeel van de paragraaf bedrijfsvoering in de p&c-documenten	Dit was een direct advies aan de gemeenteraad en valt buiten het bestek van dit klein onderzoek. Voor zover bekend is er geen opvolging aan gegeven.
ENSIA wordt ook binnen de gemeente Heusden al ruim 3 jaar als instrument gehanteerd. Dit helpt de organisatie ook nadrukkelijk bij het omvormen van de oude BIG naar BIO (zie vraag 2), en dit op een risicogerichte wijze. De afdeling I&A geeft wel aan dat het nog wel moet groeien om echt maximaal rendement uit dit instrument te halen. De rekenkamer adviseert de gemeenteraad dan ook om deze ontwikkeling actief te blijven volgen. De rekenkamer stelt voor dat het college hierover rapporteert in de tweede bestuursrapportage 2021.	Het college rapporteert via het jaarverslag en de begroting over de informatiebeveiliging. Daarnaast gebeurt dit jaarlijks met een collegeverklaring over de ENSIA audit (zie paragraaf 4.4.1).

4.7 Toekomstvastheid van het digitaal veiligheidsbeleid

De ontwikkelingen rondom digitalisering en digitale veiligheid gaan razendsnel. De opkomst van Artificiële Intelligentie (AI) heeft bijvoorbeeld weer nieuwe implicaties voor digitale veiligheid. Zo worden er door veel organisaties AI-toepassingen in werkprocessen gebruikt zonder dat er nagedacht is over de mogelijke gevolgen daarvan. Waarbij gesteld dat er met AI ook kansen liggen voor het verbeteren van digitale veiligheid.[41] Ook de gemeente Heusden staat voor de uitdaging om op deze en andere ontwikkelingen in te spelen. In deze paragraaf reflecteren we op (de controle op) de toekomstvastheid van het beleid voor digitale veiligheid in de gemeente (onderzoeksvraag 9).

De gemeente volgt actief de ontwikkelingen op het gebied van digitale veiligheid, zoals de BIO2 (de opvolger van BIO uit Box 1) en NIS2-richtlijnen[42] en treft ook maatregelen om deze veiligheid voor de toekomst te garanderen en te verbeteren waar mogelijk. Er worden op dit vlak vorderingen gemaakt (ondanks dat er nog steeds verbeterpunten zijn). Dit blijkt onder meer uit recente boardletters en accountantsverklaringen over de boekjaren 2023 en 2024.

De **Boardletter 2023** Gemeente Heusden[43] constateert dat er zichtbare verbeteringen zijn doorgevoerd in de IT-beheersmaatregelen ten opzichte van 2022. De belangrijkste bevinding ziet toe op gebruikers met superuser-rechten. In alle vier door BDO gecontroleerde applicaties (CODA, Civision, EasyInvoice en ZorgNed) beschikken meerdere medewerkers uit de lijnorganisatie over een account met verhoogde rechten (superuser-rechten).

[41] Zie [AI Trendonderzoek 2025].
[42] In het licht van alle digitale ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de *Network and Information Security (NIS2) directive.* Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet (Cbw). Op het moment dat de Cbw wordt aangenomen, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni). Zie [Cyberbeveiligingswet (NIS2-richtlijn) | Over het NCSC | Nationaal Cyber Security Centrum].
[43] BDO Audit & Assurance B.V (2024), Boardletter 2023 Gemeente Heusden.

De **Boardletter 2024** Gemeente Heusden[44] en de accountsverklaring over het boekjaar 2024 (opgesteld door BDO) benadrukken dat lokale overheden in de NIS2-richtlijnen aangewezen zijn als organisaties die van vitaal belang zijn voor de samenleving waardoor ook de gemeente Heusden verplicht is om de NIS2-maatregelen te implementeren. De belangrijkste aandachtspunten voor 2025 zien toe op het uitvoeren van een pen-test[45] en de afhankelijkheid van SaaS-leveranciers onderdeel te maken van het continuïteitsplan.[46]

BDO heeft het college erop geattendeerd om continu en grondig te evalueren of cybersecurityrisico's nog passend (juist en volledig) worden geadresseerd. BDO heeft het college drie aanbevelingen meegegeven:

1. De schematische weergave van het IT landschap verder uit te breiden met de meest kritieke systemen om zo voldoende inzicht te krijgen in het potentieel aanvalsoppervlak:
2. Periodiek security tests uit te laten voeren op het IT landschap:
3. Phishing campagnes op te zetten ter bewustwording van social enginering risico's.

Met het oog op het garanderen van digitale veiligheid in de toekomst vindt de rekenkamer het bemoedigend dat de gemeenteraad twee jaar geleden één vaste en twee tijdelijke formatieplekken heeft toegekend om de kennis en capaciteit over digitale veiligheid binnen de organisatie te vergroten. Ook ontvangen we uit onze gesprekken signalen op dat (nieuwe) medewerkers getraind worden op digitale veiligheid en bewuster en weerbaarder worden (in vergelijking met enkele jaren geleden), maar dat er bijvoorbeeld geen phishing campagnes worden gevoerd intern (tegen het advies van BDO in).

Tot slot signaleert de rekenkamer dat medewerkers behoefte hebben aan richtlijnen hoe om te gaan met nieuwe ontwikkelingen die van invloed kunnen zijn op digitale veiligheid, bijvoorbeeld inzet en gebruik van AI-tools.

[44] Zie [Document Heusden - 20250617 BIJL2 Boardletter 2024 - iBabs Publieksportaal].
[45] Een pen-test is een gesimuleerde cyberaanval van een ethische hacker om de beveiliging van een systeem of netwerk te testen. Het doel is om zwakke plekken en kwetsbaarheden te identificeren voordat kwaadwillende hackers ze kunnen misbruiken. Zie [Voer een pentest uit tegen cybercirme - Het CCV].
[46] BDO Audit & Assurance B.V. (2025), Accountantsverslag 2024 Gemeente Heusden, p. 13.

5. Conclusies en aanbevelingen

5.1 Conclusies

Op basis van dit onderzoek komt de rekenkamer tot de volgende conclusies:

Hoofdconclusie digitale veiligheid

De gemeente Heusden heeft in de afgelopen jaren een solide basis gelegd voor digitale veiligheid met een compleet en actueel beleidskader en de benodigde organisatorische structuur. Dit heeft geleid tot aantoonbare verbeteringen en een beheersbaar incidentenniveau. Om de toekomstbestendigheid en doeltreffendheid van dit beleid verder te waarborgen, is het cruciaal dat de gemeente de beleidskaders operationeel volledig uitwerkt en vastlegt, de bewustwording en het gedrag van medewerkers traint en achterstanden in risicomanagement proactief wegwerkt, terwijl zij voortdurend alert blijft op nieuwe dreigingen en noodzakelijke testen uitvoert.

Beleidskaders en organisatie

1. De rekenkamer stelt vast dat de gemeente Heusden een compleet en actueel beleidskader heeft voor het bevorderen en bewaken van digitale veiligheid en dat dit beleidskader tevens landelijke richtlijnen hieromtrent volgt en – voor zover dit beknopt onderzoek daar zicht op heeft - naleeft.
2. De rekenkamer stelt vast dat de gemeente Heusden in de interne organisatie beschikt over de relevante functionarissen die het beleid en de maatregelen voor digitale veiligheid sturen, ontwikkelen, uitvoeren en monitoren.
3. De rekenkamer stelt vast dat de gemeente Heusden dit beleidskader nog niet volledig heeft uitgewerkt en vastgesteld in operationele werkplannen en -instructies.
4. De rekenkamer stelt vast dat de evaluatie van het beleid informatiebeveiliging en privacy 2024-2028 besproken in het MT en vastgelegd wordt in de notulen van het MT. De notulen van het MT kunnen volgens ons niet beschouwd worden als een formeel evaluatieverslag.

Betrokkenheid van de bredere organisatie

5. De rekenkamer stelt vast dat digitale veiligheid (en aanverwante onderwerpen) in zowel het college als het managementteam aan de orde komen en dat de functionarissen die verantwoordelijk zijn voor de ontwikkeling en uitvoering van dit beleid zich gesteund voelen.
6. De rekenkamer stelt vast dat de gemeente Heusden het belang van digitale veiligheid goed onder de aandacht brengt bij alle medewerkers. Het vergroten en onderhouden van kennis, houding en gedrag op dit vlak heeft echter een bescheiden en vrijwillig karakter (sterke nadruk op Sir Askalot).

Testen, audits en resultaten

7. De rekenkamer stelt vast dat de gemeente Heusden periodiek zowel interne als externe testen en audits verricht en dat deze tot dusver geen grote of acute knelpunten hebben blootgelegd ten aanzien van digitale veiligheid. De betrokken functionarissen zijn zich ook bewust van het belang van testen en audits.

Beleidskaders en organisatie

8. De rekenkamer stelt vast dat de gemeente Heusden zich via verschillende (landelijke) kanalen laat informeren over mogelijke risico's ten aanzien van digitale veiligheid.
9. De rekenkamer stelt vast dat de gemeente Heusden achterstand dreigt op te lopen bij het zo goed mogelijk garanderen van digitale veiligheid bij (nieuwe) digitale processen en applicaties, onder meer vanwege de opgelopen achterstand met het uitvoeren van Data Protection Impact Assessments en opruimacties van oude mailberichten en documenten.
10. De rekenkamer stelt vast dat het aantal en de intensiteit van incidenten tot dusver behandelbaar zijn geweest. Er is geen trend te ontwaren.

Opvolging van aanbevelingen uit de rekenkamerbrief "Digitale veiligheid in tijden van corona"

11. De rekenkamer stelt vast dat de gemeente Heusden opvolging heeft gegeven aan enkele aanbevelingen, onder meer over ENSIA en bij andere aanbevelingen valide beargumenteert waarom deze niet zijn overgenomen, onder meer ten aanzien van de keuzevrijheid van raadsleden.
12. De rekenkamer constateert dat raadsleden geen doelgroep van het beleid ten aanzien van digitale veiligheid van de gemeente Heusden zijn geworden, omdat de raadsleden geen toegang hebben tot of gebruik maken van de (interne) bedrijfsvoeringsystemen van de gemeente.

Toekomstvastheid van het digitale veiligheidsbeleid

13. De rekenkamer stelt vast dat de accountant zichtbare verbeteringen ziet in de IT-beheersmaatregelen ten opzichte van 2022. Dit bevestigt het beeld dat er belangrijke stappen vooruit zijn gezet (actuele en complete beleidskader, bewustwording en training van medewerkers, meer sturen op digitale veiligheid bij aanschaf/huur van nieuwe applicaties).
14. De rekenkamer stelt vast dat de accountant relevante aanbevelingen doet voor het mitigeren van risico's in het domein van digitale veiligheid.
15. De rekenkamer ondersteunt de conclusie van de accountant dat de gemeente een pen-test kan laten uitvoeren; ook omdat we op basis van dit onderzoek constateren dat de gemeente de digitale veiligheid weinig test aan de hand van bijvoorbeeld een gesimuleerde phishing-mail.
16. De rekenkamer stelt vast dat het beleid ten aanzien van digitale veiligheid voldoende toekomstbestendig is, maar dat er op korte termijn wel enkele plannen en assessments afgerond dienen te worden, zoals de tactische en operationele uitwerking van het Beleid informatiebeveiliging en privacy 2024-2028 Gemeente Heusden, *data protection impact assessments* en een beoordelingsproces voor het identificeren en aanpakken van risico's die samenhangen met persoonsgegevens.
17. De rekenkamer stelt vast dat digitaal veiligheidsbeleid nooit af is. Nieuwe ontwikkelingen, bijvoorbeeld artificiële intelligentie, vergen een regelmatige herijking en aanpassing van dit beleid (en de uitwerking daarvan).

5.2 Aanbevelingen

Op basis van dit onderzoek komt de rekenkamer tot de volgende vier aanbevelingen:

1. **Versterk en complementeer de interne uitwerking van de beleidskaders voor digitale veiligheid**. Hoewel de beleidskaders compleet en actueel zijn, ontbreekt het nog aan de volledige operationele uitwerking en vastlegging. Zorg dat alle toekomstige evaluaties, inclusief die van het beleid informatiebeveiliging en privacy, worden vastgelegd in een

afzonderlijk evaluatieverslag. Dit zorgt voor aantoonbaarheid, consistentie en overdraagbaarheid van kennis.

2. **Intensiveer training voor en bewustwording van digitale veiligheid.** Blijf investeren in het vergroten en onderhouden van kennis, houding en gedrag op het gebied van digitale veiligheid voor *alle* medewerkers en dat bij voorkeur met een verplicht programma. Dit is meer dan deelname aan *Sir Askalot* en de training van nieuwe medewerkers door het team Informatie & Privacy (team I&P). Overweeg gesimuleerde aanvallen (bijvoorbeeld een phishing-mail of pen-test) om de bewustwording en weerbaarheid van medewerkers (in het echt) te testen en te vergroten.
3. **Elimineer achterstanden bij het risicobeheer**. Er dreigt achterstand bij het waarborgen van digitale veiligheid bij nieuwe processen en applicaties, met name door de achterstand in *Data Protection Impact Assessments (DPIA's)* en het opschonen van oude data (verouderde e-mails en bestanden). Geef prioriteit aan het uitvoeren van alle openstaande DPIA's voor nieuwe en bestaande digitale processen en applicaties. Start of versnel opruimacties van oude mailberichten en documenten om risico's te mitigeren en compliance te verbeteren.
4. **Blijf proactief innoveren en controleren.** Het bewaken en bevorderen van digitale veiligheid is een continu proces dat nooit af is. Het is essentieel om alert te blijven op nieuwe risico's en technologieën. Integreer een proces voor de regelmatige herijking en aanpassing van het digitale veiligheidsbeleid op basis van nieuwe technologische ontwikkelingen, zoals artificiële intelligentie.

6. Bestuurlijke reactie

Rekenkamer Heusden

ONS KENMERK: 2126924
UW KENMERK:
UW BRIEF VAN: 1 september 2025
BEHANDELD DOOR:
ONDERWERP: bestuurlijk wederhoor m.b.t. onderzoek Digitale veiligheid in de gemeente Heusden
AANTAL BIJLAGEN:
DATUM: 8 september 2025
VERZ. 9 september 2025

Beste leden van de Rekenkamer,

Wij hebben met belangstelling uw onderzoeksrapport ‘Is de gemeente Heusden digitaal veilig?’ gelezen. U verzoekt om een bestuurlijke reactie. Met deze brief geven we deze reactie.

Allereerst danken wij u voor de inzichten die het onderzoek biedt op een onderwerp dat in deze roerige, digitale tijden ons allen raakt. Digitale veiligheid is een randvoorwaarde om inwoners goed en betrouwbaar van dienst te zijn. Het sluit aan bij onze kernwaarden om de klant centraal te stellen, samen te werken en de dialoog aan te gaan, elkaar aan te spreken en verantwoordelijkheid te nemen, en draagt bij aan de ambitie uit het coalitieprogramma Heusden Nu en Straks om te bouwen aan een moderne en toekomstbestendige overheid.

We zijn dan ook verheugd te lezen dat u het volgende concludeert: ‘de gemeente Heusden heeft in de afgelopen jaren een solide basis gelegd voor digitale veiligheid met een compleet en actueel beleidskader en de benodigde organisatorische structuur. Dit heeft geleid tot aantoonbare verbeteringen en een beheersbaar incidentenniveau’. Deze solide basis is mede te danken aan de inzet van twee tijdelijke functies, waardoor we de afgelopen periode meer menskracht hebben gehad in zowel beleid als uitvoering. In de voorjaarsnota zal een integrale afweging worden gemaakt ten aanzien van noodzakelijke formatiebehoefte.

Ook wij beseffen heel goed dat digitale veiligheid nooit een eindpunt kent maar voortdurend in ontwikkeling is. We volgen daarom de technische ontwikkelingen op de voet en nemen aanbevelingen mee om onze aanpak steeds verder te versterken.

Graag maken wij van deze gelegenheid gebruik om op uw aanbevelingen te reageren.

Aanbeveling 1. Versterk en complementeer de interne uitwerking van de beleidskaders voor digitale vaardigheid.

Hoewel de beleidskaders compleet en actueel zijn, ontbreekt het nog aan de volledige operationele uitwerking en vastlegging. Zorg dat alle toekomstige evaluaties, inclusief die van het beleid informatiebeveiliging en privacy, worden vastgelegd in een afzonderlijk evaluatieverslag. Dit zorgt voor aantoonbaarheid, consistentie en overdraagbaarheid van kennis.

Deze aanbeveling nemen wij over. De jaarlijkse evaluatie van het beleid informatiebeveiliging en privacy zal voortaan worden vastgelegd in een afzonderlijk evaluatieverslag. Ook voor de overige beleidsstukken zal worden gekeken naar een passende evaluatiemethode.

Aanbeveling 2. Intensiveer training voor en bewustwording van digitale veiligheid.

Blijf investeren in het vergroten en onderhouden van kennis, houding en gedrag op het gebied van digitale veiligheid voor alle medewerkers en dat bij voorkeur met een verplicht programma. Dit is meer dan deelname aan

Sir Askalot en de training van nieuwe medewerkers door het team Informatie & Privacy (team I&P). Overweeg gesimuleerde aanvallen (bijvoorbeeld een phishing-mail of pen-test) om de bewustwording en weerbaarheid van medewerkers (in het echt) te testen en te vergroten.

Deze aanbeveling nemen we over.

Aanbeveling 3. Elimineer achterstanden bij het risicobeheer.

Er dreigt achterstand bij het waarborgen van digitale veiligheid bij nieuwe processen en applicaties, met name door de achterstand in Data Protection Impact Assessments (DPIA's) en het opschonen van oude data (verouderde e-mails en bestanden). Geef prioriteit aan het uitvoeren van alle openstaande DPIA's voor nieuwe en bestaande digitale processen en applicaties. Start of versnel opruimacties van oude mailberichten en documenten om risico's te mitigeren en compliance te verbeteren.

Onze gemeentelijke organisatie werkt voortdurend aan het verbeteren van de informatiehuishouding. Dit draagt bij aan het verminderen van risico's en het voldoen aan wet- en regelgeving. Daarom loopt er op dit moment een project waarin digitale samenwerkingsverbanden worden gemoderniseerd door middel van Microsoft Teams. Met dit project creëren we randvoorwaarden voor het opschonen van bestanden en het duurzaam beheren van informatie. Alle huidige documentatie wordt bekeken en opgeruimd, wat aansluit bij uw advies.

Ook nemen we de aanbeveling over voor het prioriteren van het uitvoeren van Data Protection Impact Assesments (DPIA) bij nieuwe en bestaande processen en applicaties. Er is al een plan van aanpak gemaakt door de Privacy Officer om de achterstanden te gaan inlopen.

Aanbeveling 4. Blijf proactief innoveren en controleren.

Het bewaken en bevorderen van digitale veiligheid is een continu proces dat nooit af is. Het is essentieel om alert te blijven op nieuwe risico's en technologieën. Integreer een proces voor de regelmatige herijking en aanpassing van het digitale veiligheidsbeleid op basis van nieuwe technologische ontwikkelingen, zoals artificiële intelligentie.

Wij erkennen dat digitale veiligheid een continu proces is dat blijvende alertheid vraagt. We spelen hierop in door ontwikkelingen zoals artificiële intelligentie actief te volgen en waar nodig te vertalen naar beleid en praktijk. Daarnaast sluiten we met de collectieve aanbesteding Cyberweerbaarheid van de VNG nadrukkelijk aan op de noodzaak van preventie en voortdurende herijking, zodat onze digitale veiligheid meebeweegt met nieuwe risico's en ontwikkelingen.

Tot slot

Wij zijn dankbaar voor de inzichten in dit rekenkameronderzoek, die helpen om de digitale veiligheid steeds te blijven ontwikkelen.

Met vriendelijke groet,
het college van Heusden,

de secretaris,	de burgemeester,
Mr. HJM Timmermans	drs. W. van Hees

Bijlage 1. Lijst gesprekspartners

- Beleidsmedewerker Kunst en Cultuur (10 juli 2025)
- Beleidsmedewerker Regionale samenwerking (10 juli 2025)
- Beleidsmedewerker Sociaal Domein (10 juli 2025)
- Chief Information Security Officer (CISO) (11 juni 2025)
- Clustermanager Informatisering & Automatisering (I&A) (10 juni 2025)
- Coördinator Burgerzaken/Klantencontactcentrum (10 juli 2025)
- Privacy Officer (25 juni 2025)
- Senior adviseur bedrijfsvoering (10 juli 2025)

Bijlage 2. Normenkader

Nr.	Norm	Voldoet
1	De gemeente Heusden beschikt over een actueel en compleet beleidskader voor de borging van digitale veiligheid.	Ja, maar vergt op onderdelen tactische en operationele uitwerking. Zie paragraaf 2.2.
2	De gemeente Heusden heeft een vervolg gegeven aan de aanbevelingen uit de rekenkamerbrief “Digitale veiligheid in tijden van corona” (of minimaal beargumenteerd waarom zij dat niet heeft gedaan).	Ja, enkele aanbevelingen zijn opgevolgd (bijvoorbeeld over ENSIA). Zie paragraaf 2.6.
3	De gemeente Heusden voldoet aan de bepalingen van de Baseline Informatiebeveiliging Overheid (BIO).	Ja, voor zover dit beperkt onderzoek dat toelaat, stellen wij vast dat de gemeente zich conformeert aan BIO. Zie paragraaf 2.2.
4	De gemeente Heusden voert een actief beleid ten aanzien van digitale veiligheid en dat zowel gericht op kennis, houding en gedrag van medewerkers als op (technische) infrastructuur.	Ja, medewerkers worden op vrijwillige basis getraind in kennis, houding en gedrag ten aanzien van digitale veiligheid. Zie paragraaf 2.3
5	De gemeente Heusden is zich bewust van de mogelijke risico’s in de huidige wijze waarop digitale veiligheid is ingericht en functioneert.	Ja, de gemeente laat met regelmaat interne en externe audits uitvoeren. Zie paragrafen 2.4 en 2.5
6	De gemeente Heusen ziet erop toe dat digitaal veiligheidsbeleid van een voldoende niveau is en blijft en dat er wordt geanticipeerd op toekomstige opgaven.	Ja, de gemeente evalueert het beleid, volgt landelijke richtlijnen en inventariseert nieuwe risico’s. Zie paragraaf 2.7.
7	De gemeente Heusden registreert (digitale) beveiligingsincidenten, heeft haar ‘incident response’ op orde en leert uit ervaringen.	Ja, de gemeente registreert incidenten, verbetert haar incident response en trekt lering uit ervaringen. Zie paragraaf 2.6.

Gemeente Heusden

Julianastraat 34
5251 ED Vlijmen

Postbus 41
5250 AA Vlijmen

(073) 513 17 99
(06) 53 235 705 (Whatsapp)
www.heusden.nl