Rekenkamer gemeente Oude IJsselstreek

VEILIGHEID VERTROUWD!?

Rekenkameronderzoek naar Informatiebeveiliging en Privacy

Versie:	Definitief
Datum:	16 juni 2025
Vertrouwelijkheid:	Bedrijfsvertrouwelijk

Inhoudsopgave

1. Voorwoord 3
1.1 Inleiding 3
1.2 Onderzoeksvragen 3
1.3 Onderzoeksmethodiek 4
1.5 Leeswijzer 4
1.6 Dankwoord 5
2. De Mens 6
2.1 Mail phishing 6
2.2 Voice phishing 6
2.3 Inlooptest 6
2.4 Enquête 7
3. De Techniek 13
3.1 Penetratietest op de externe infrastructuur 13
3.2 Penetratietest op de interne infrastructuur 13
3.3 Penetratietest op het beveiligde Wifi-netwerk 14
4. De Organisatie 15
4.1 Toets normenkaders informatiebeveiliging en privacy 15
4.2 Aanvullende bevindingen uit de interviews 18
5. Conclusies 20
6. Aanbevelingen 22

Bijlage 1: Bestuurlijke reactie 23
Bijlage 2: Nawoord rekenkamer 29
Bijlage 3: Verklarende woordenlijst 30
Bijlage 4: Onderzoeksverantwoording 31
A) De Mens 31
B) De Techniek 32
C) De Organisatie 32
D) Normenkader 32
E) Transparantieparagraaf 34
Bijlage 5: Geraadpleegde bronnen 35
A) Documenten 35
B) Interviews en praktijkcasussen 36
Bijlage 6: Uitgezette enquête 37

1. Voorwoord

1.1 Inleiding

Het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de door de gemeente beheerde informatie en data is een basistaak geworden. Als gevolg van de decentralisaties binnen het sociaal domein (Wmo, jeugdzorg en participatie) is het aantal door de gemeente beheerde bijzondere persoonsgegevens daarnaast sterk gegroeid. Samen met gegevens die de gemeente daarvoor al tot haar beschikking had, is het beveiligen van de toegang tot, het gebruik en het verstrekken van deze data essentieel geworden.

Door keten- en netwerksamenwerking ontvangt en deelt de gemeente veel van deze data en informatie. Door de digitalisering van de maatschappij en de gangbare norm van tijd- en plaatsonafhankelijke toegang tot data, zijn privacybescherming en beveiliging van deze data en informatie een 24/7 verantwoordelijkheid.

De kans op ongeautoriseerde toegang tot en misbruik van deze data en informatie is de afgelopen jaren groter geworden. Bijna dagelijks zijn er bij gemeenten (pogingen tot) cyberaanvallen, verstoringen van de informatiebeveiliging of andere (bijna) incidenten. Het gaat hierbij om aanvallen van buitenaf via internet of e-mail (bv. via phishing mails of gijzelingsvirussen), onveilige verbindingen en links, virussen via besmette bestanden/computers e.d. waardoor computers, systemen en bestanden overgenomen, afgeluisterd, geblokkeerd, versleuteld of beschadigd kunnen worden. Ook gaat het om eventuele informatielekken van binnenuit (al dan niet moedwillig) en onveilig omgaan met gegevens(dragers) c.q. oneigenlijk gebruik van bestanden en (vertrouwelijke) gemeentelijke gegevens.

De impact van een beveiligingsincident kan zeer groot zijn. De afgelopen jaren zijn in de directe omgeving van de gemeente Oude IJsselstreek nieuwswaardige incidenten geweest. Denk hierbij aan de datadiefstallen bij de GGD in januari 2021 tijdens de coronapandemie, de hacks of pogingen daartoe bij de gemeenten Lochem en Hof van Twente in 2019 en 2020 en van de Veiligheidsregio Noord en Oost-Gelderland in september 2020.

De verantwoordelijkheid die de overheid draagt voor de fysieke veiligheid zou in gelijke mate moeten gelden voor de digitale veiligheid. Burgers, bedrijven en organisaties moeten erop kunnen vertrouwen, dat hun gegevens in goede handen zijn bij de overheid. Dat is de essentie van het vertrouwen dat men in de overheid moet kunnen stellen.

Het beveiligen van (digitale) informatie en het bewaken van de privacy is van een ICT-vraagstuk veranderd in een bestuurlijk relevant onderwerp. Daarmee is het ook een verantwoordelijkheid van de gemeenteraad geworden, die kaders zou moeten stellen en het college moet controleren op het uitvoeren van zijn taken op dit gebied. Het is belangrijk om ook als gemeenteraad goed bij dergelijke belangrijke strategische kwesties betrokken te zijn.

De rekenkamer geeft met het uitgevoerde onderzoek naar informatiebeveiliging en privacy de gemeenteraad inzicht in:

1. De doeltreffendheid van het actuele informatiebeveiligings- en privacybeleid en de bijbehorende beheersmaatregelen.
2. De eventuele risico's die de gemeente loopt op het gebied van informatiebeveiliging en privacy intern en in samenwerkingsverbanden (gedeelde ICT-voorzieningen).
3. De impact van toekomstige opgaven (zoals Artificial Intelligence (AI), datagedreven werken en Europese eisen) op het gebied van informatiebeveiliging en privacy.

1.2 Onderzoeksvragen

Om tot deze inzichten te komen is de volgende centrale onderzoeksvraag gedefinieerd:

Is de informatiebeveiliging en privacybescherming van de gemeente Oude IJsselstreek – mede in relatie tot samenwerkingsverbanden – doeltreffend en doelmatig ingericht?

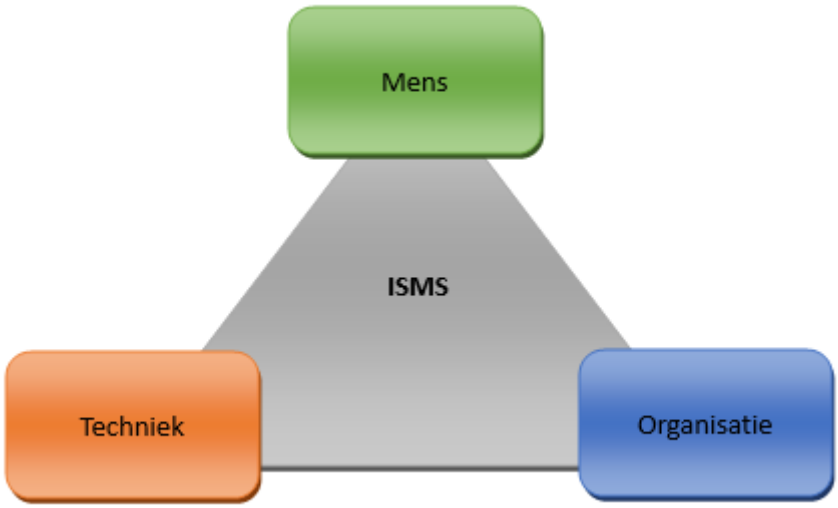
In de kern is het de zoektocht naar de vraag of de gemeente Oude IJsselstreek een goed beeld heeft van de belangrijkste risico's op het gebied van informatiebeveiliging en specifiek de privacybescherming van gevoelige informatie zoals (bijzondere) persoonsgegevens.

Om deze centrale vraag te kunnen beantwoorden definiëren we de volgende deelvragen:

1. Heeft de gemeente op een adequate manier invulling gegeven aan haar informatiebeveiligings- en privacybeleid?
2. In hoeverre is de sturing van de gemeente binnen samenwerkingsverbanden toereikend op het gebied van informatiebeveiliging en privacy?
3. In hoeverre zijn risico's en beheersmaatregelen (intern en binnen samenwerkingsverbanden) in kaart gebracht en op welke wijze worden deze consequent opgevolgd?
4. Op welke wijze anticipeert de gemeente op toekomstige ontwikkelingen (die invloed hebben) op het gebied van informatiebeveiliging en privacy?
5. Hoe wordt de gemeenteraad betrokken bij de thema's informatiebeveiliging en privacy?

1.3 Onderzoeksmethodiek

Informatiebeveiliging en privacy zijn via drie 'velden' met elkaar verbonden en vormen gezamenlijk het zogeheten Informatie Beveiligings Management Systeem (in het Engels: ISMS). Visueel weergegeven ziet dat er als volgt uit:



Om tot een goed antwoord op de centrale onderzoeksvraag te komen zijn alle drie de velden apart onderzocht. Een nadere toelichting op de onderzoeksmethodiek is opgenomen in bijlage 4.

1.5 Leeswijzer

Deze rapportage start met een samenvatting van de belangrijkste constateringen uit dit onderzoek. Hierna wordt aan de hand van de onderzoekscomponenten 'De Mens', 'De Techniek' en 'De Organisatie', een antwoord gegeven op de onderzoeksvragen. Het rapport sluit af met de conclusies en de aanbevelingen.

De rekenkamer heeft getracht deze rapportage in voor een leek begrijpelijke taal te schrijven. Gezien het onderzoeksonderwerp kunnen bepaalde vaktermen niet voorkomen worden. Hierom zijn in de bijlagen onder andere een verklarende woordenlijst opgenomen, evenals een onderzoeksverantwoording en een overzicht van geraadpleegde bronnen.

Aanvullend zijn gegevens en bevindingen die naar hun aard vertrouwelijk zijn, niet in deze rapportage opgenomen.

1.6 Dankwoord

Bij de uitvoering van dit onderzoek is constructieve medewerking verleend door de ambtelijke organisatie en het gemeentebestuur. Door de snelle aanlevering van een grote hoeveelheid aan uitgevraagde documenten, de veelvuldig ingevulde digitale vragenlijst en de medewerking aan diverse interviews heeft de rekenkamer binnen de beoogde planning haar onderzoek uit kunnen voeren.

De rekenkamer dankt eenieder voor haar medewerking en daarmee ieders bijdrage aan de voorliggende eindrapportage.

2. De Mens

De mens is doorgaans de zwakste schakel bij het borgen van de informatiebeveiliging en privacy. Hierom is in het rekenkameronderzoek specifiek aandacht besteed aan het menselijk gedrag. In dit onderzoek is de factor mens op vier verschillende manieren onderzocht:

1. Mail phishing
2. Voice phishing
3. Inlooptest
4. Enquête

Een toelichting op deze vier onderzoeksmethodieken is beschreven in bijlage 4. In het vervolg van dit hoofdstuk worden de onderzoeksresultaten van deze 4 methodieken nauwkeurig beschreven.

2.1 Mail phishing

Onderzoeksbureau NFIR heeft tussen 23 en 30 september 2024 een mailphishing campagne uitgezet onder alle medewerkers (inclusief ingehuurde medewerkers), de leden van het College van B&W, de leden van de gemeenteraad en fractieassistenten (totaal 561 medewerkers).

In totaal hebben 72 medewerkers op de link in de phishingmail geklikt (13%), waarvan 35 medewerkers daadwerkelijk hun gebruikersnaam en wachtwoord hebben gedeeld (6%). Het NFIR heeft geen wachtwoorden opgeslagen. Indien het een malafide mailphishing betrof (in tegenstelling tot deze test) dan was via 35 medewerkers gedeeltelijke toegang tot systemen van de gemeente mogelijk geweest.

Het aantal medewerkers dat geklikt heeft op de phishingmail en het aantal medewerkers dat vervolgens daadwerkelijk gegevens heeft achtergelaten is relatief laag. Uit landelijk onderzoek van het Ministerie van Justitie en Veiligheid en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties uit januari 2024 naar phishing onder 1033 respondenten, blijkt dat gemiddeld 1 op 10 Nederlanders op een malafide link klikt en ongeveer de helft daarvan ook daadwerkelijk gegevens achterlaat[1]. Daarmee is het resultaat in Oude IJsselstreek vergelijkbaar met het landelijk gemiddelde.

2.2 Voice phishing

Onderzoeksbureau NFIR heeft 16 medewerkers geprobeerd te bereiken voor een voice phishing. Uiteindelijk zijn 6 medewerkers gesproken, waarvan 3 medewerkers (50%), daadwerkelijk gebruikersnaam en wachtwoord hebben achtergelaten op de website waarnaar verwezen werd. Eén gebelde medewerker vertrouwde het niet en heeft de CISO geïnformeerd.

De medewerkers die gegevens hebben achtergelaten zijn geïnformeerd dat dit een test betrof en hoe ze konden achterhalen dat dit een voice phishing campagne betrof. Zo werd er anoniem gebeld, waarbij de afdeling ICT altijd met nummerherkenning belt.

2.3 Inlooptest

Op 24 september 2024 heeft een medewerker van het NFIR geprobeerd toegang te krijgen tot zowel het gemeentehuis (Staringstraat 25) als bij STOER in de DRU in Ulft. Dit heeft verschillende resultaten opgeleverd. Voor het gemeentehuis geldt dat:

- Toegang verkregen kon worden via de personeelsingang, het werkcafé en de receptie.
- De medewerker van het NFIR bij toegang via de personeelsingang (door mee te lopen met legitieme medewerkers) tot drie keer toe door medewerkers vriendelijk is aangesproken en gecontroleerd is op geautoriseerde toegang. Hierbij heeft de medewerker van het NFIR zijn 'vrijkaart' moeten tonen.
- In het werkcafé heeft de medewerker van het NFIR een vertrouwelijk gesprek mee kunnen luisteren van een lid van de ondernemingsraad.
- Er was via de receptie geen mogelijkheid voor toegang tot de medewerkersgangen. Deze zaten allemaal op slot en de medewerker van het NFIR kon niet meelopen met iemand.

[1] Zie: Misleidende online berichtgeving

- Er waren geen documenten aanwezig bij de printers en er konden geen printopdrachten uit de printers gehaald worden.
- Het was mogelijk om de eigen laptop bekabeld aan te sluiten op het netwerk van de gemeente. Hierbij werd een IP-adres toegekend in het gastennetwerk.
- De bezemkast was niet afgesloten. Een insluiper zou zich hier kunnen verstoppen.

Voor toegang tot STOER in de DRU geldt het volgende:

- De medewerker van het NFIR werd toegelaten door een medewerker van STOER (deur werd geopend) na aangegeven te hebben dat hij een medewerker van de gemeente was.
- De medewerker van het NFIR kon vrij rondlopen bij STOER en is door niemand aangesproken.
- Ongewenste bezoekers worden niet gedetecteerd of begeleid.
- In de DRU kon de medewerker van het NFIR een sollicitatiegesprek afluisteren.

2.4 Enquête

De enquête is door 272 ontvangers geopend en door 195 ontvangers volledig ingevuld. Op een totaal van 493 ontvangers (inclusief gemeenteraadsleden en fractieassistenten) betekent dit dat bijna 40% van de aangeschreven respondenten de enquête heeft ingevuld. Voor de analyse van de resultaten zijn enkel de 195 volledig ingevulde enquêtes meegenomen.

Door alle afdelingen is de enquête ingevuld:

Afdeling	Aantal medewerkers	Aantal ingevulde enquêtes	% ingevuld
Bedrijfsvoering	101	42	41,6%
BUOR	85	22	25,9%
College van Burgemeester en Wethouders	6	4	66,7%
Concernstaf	19	11	57,9%
Fysieke ontwikkeling	69	28	40,6%
Gemeenteraad (en fractieassistenten)	57	19	33,3%
Griffie	4	2	50,0%
Publiekszaken, Economie en Maatschappij (PEM)	57	23	40,4%
Sociaal Domein	95	44	46,3%
Totaal	**493**	**195**	**39,6%**

De belangrijkste vraag in de enquête betrof in hoeverre men zich houdt aan de gedragsregels op het gebied van informatiebeveiliging en privacy. Op basis van de 195 ingevulde enquêtes ontstaat het volgende totaalbeeld in absolute aantallen (en percentueel):

Gedragsregel	Is dit een gedragsregel?	Oei, die was ik vergeten; ik moet daar beter op gaan letten	Ik pas deze regel soms toe	Ik pas deze regel meestal toe	Dit doe ik altijd	Deze regel is op mijn werkzaamheden niet van toepassing	Totaal
1. Een informatiebeveiligings- en/of privacy-incident meld ik via het beschikbare meldformulier	20 (10,3%)	21 (10,8%)	20 (10,3%)	32 (16,4%)	82 (42,1%)	20 (10,3%)	**195 (100%)**
2. E-mails met (bijzondere) persoonsgegevens en/of vertrouwelijke/gevoelige data	11 (5,6%)	16 (8,2%)	12 (6,2%)	53 (27,2%)	75 (38,5%)	28 (14,4%)	**195 (100%)**

verstuur ik altijd via de beveiligde mailoplossing Bastion365							
3. Ik volg jaarlijks het bewustwordingsprogramma informatiebeveiliging en privacy	52 (26,7%)	31 (15,9%)	8 (4,1%)	20 (10,3%)	67 (34,4%)	17 (8,7%)	**195 (100%)**
4. Mijn werklaptop gebruik ik in principe niet voor privédoeleinden	11 (5,6%)	1 (0,5%)	14 (7,2%)	61 (31,3%)	100 (51,3%)	8 (4,1%)	**195 (100%)**
5. Ik vergrendel mijn scherm als ik mijn werkplek verlaat	8 (4,1%)	14 (7,2%)	25 (12,8%)	61 (31,3%)	85 (43,6%)	2 (1,0%)	**195 (100%)**
6. Ik zorg dat op mijn werkplek geen gevoelige/vertrouwelijke informatie ligt als ik mijn werkplek verlaat	1 (0,5%)	3 (1,5%)	17 (8,7%)	64 (32,8%)	103 (52,8%)	7 (3,6%)	**195 (100%)**
7. Ik zorg ervoor dat anderen mijn vertrouwelijke / gevoelige gesprekken niet mee kunnen luisteren (zowel op kantoor, thuis als in het openbaar).	2 (1,0%)	0 (0,0%)	17 (8,7%)	59 (30,3%)	107 (54,9%)	10 (5,1%)	**195 (100%)**
8. Grote bestanden verstuur ik veilig met Bastion365	24 (12,3%)	12 (6,2%)	19 (9,7%)	33 (16,9%)	48 (24,6%)	59 (30,3%)	**195 (100%)**
9. In e-mailberichten open ik geen onbekende url's of bijlagen. Ik vul geen gegevens in bij een (onverwacht) bericht met onbekende afzender.	2 (1,0%)	0 (0,0%)	4 (2,1%)	21 (10,8%)	165 (84,6%)	3 (1,5%)	**195 (100%)**
10. Ik maak geen gebruik van openbare Wifi-netwerken (toegang tot Wifi zonder wachtwoord)	8 (4,1%)	11 (5,6%)	18 (9,2%)	43 (22,1%)	109 (55,9%)	6 (3,1%)	**195 (100%)**

Hieronder staat per regel een toelichting:

1. Een informatiebeveiligings- en/of privacy-incident meld ik via het beschikbare meldformulier.

In het informatiebeveiligingsbeleid is als één van de strategische uitgangspunten '*Alle medewerkers melden veiligheidsincidenten, op incidenten wordt opvolging gegeven'* opgenomen. Het is hierom opvallend dat 10,3% van de respondenten aangeeft dat deze regel op hun werkzaamheden niet van toepassing is. Uitgaande van het beleid zou dit 0% moeten zijn.

Tevens is opvallend dat deze regel door 10,3% van de respondenten niet herkend wordt. Het totaalbeeld laat zien dat minder dan de helft (42,1%) van de respondenten een incident altijd meldt.

Bij de toelichting die gegeven kon worden op deze regel komt samengevat het volgende terug:

- Een deel van de respondenten is niet bekend hoe ze moeten melden en wat meldingswaardig is.
- Een deel van de respondenten doet zelf een risico-inschatting van een incident en daarmee of het meldingswaardig is.
- Het invullen van het meldformulier kost veel tijd.
- Er komt niet altijd een terugkoppeling op de melding, waardoor een deel van de respondenten het idee krijgt dat de melding niet nuttig was.
- Externen zijn niet geattendeerd op de meldingsprocedure.

2. E-mails met (bijzondere) persoonsgegevens en/of vertrouwelijk/gevoelige data verstuur ik altijd via de beveiligde mailoplossing Bastion365.

In het informatiebeveiligingsbeleid is opgenomen dat '*Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie'.* Sinds 28 februari 2024 is voor het verzenden van dit soort gegevens Bastion365 organisatiebreed beschikbaar gesteld.

Uit de enquête blijkt dat respondenten deze regel meestal (27,2%) of altijd (38,5%) toepassen. Respondenten die niet met dit soort gegevens werken geven logischerwijs aan dat deze regel niet op hen van toepassing is (14,4%).

De respondenten die deze regel vergeten waren, er niet bekend mee waren of soms toepassen, onderbouwen dit als volgt:

- Het gebruik van Bastion365 wordt als vertragend en omslachtig ervaren.
- Het verplichte 06-nummer van de geadresseerde is niet altijd bekend, waardoor vertrouwelijke gegevens toch via reguliere mail verzonden worden.
- Er is geen uitleg gegeven over het gebruik van Bastion365 waardoor de tool niet gebruikt wordt.
- De snelheid van handelen en ervaren werkdruk maken dat Bastion365 wordt overgeslagen.
- Bastion365 werkt niet altijd waardoor voor de reguliere verzendwijze wordt gekozen.

3. Ik volg jaarlijks het bewustwordingsprogramma informatiebeveiliging en privacy.

In het informatiebeveiligingsbeleid is als één van de strategische uitgangspunten opgenomen dat *'alle medewerkers doen jaarlijks mee met de bewustzijnstrajecten. Meervoudig niet meedoen kan worden gezien als werkweigering en kan dus leiden tot aantekeningen in het personeelsdossier. Met de bewustzijnstrajecten worden de risico's van menselijk gedrag geminimaliseerd.'*

Opvallen in de ingevulde enquête is dat 8,7% van de respondenten aangeeft dat deze regel op hen niet van toepassing is. Conform het beschreven strategische uitgangspunt zou dit niet mogen; het meedoen aan de jaarlijkse bewustzijnstrajecten is immers voor alle medewerkers.

Iets meer dan één derde van de respondenten (34,4%) geeft aan jaarlijks het bewustzijnsprogramma te volgen. De overige respondenten kenden deze regel niet of letten hier niet op. Respondenten onderbouwen dit als volgt:

- Er is respondenten door hun manager of door de CISO of FG nooit verteld dat het volgen van een dergelijk programma verplicht is.
- Bij een deel van de respondenten is niet bekend dat er een dergelijk jaarlijks bewustzijnsprogramma is.
- Bij een deel van de respondenten ontbreekt het aan tijd om het programma te volgen.
- Een deel van de respondenten geeft aan dat informatie via het intranet wordt gepubliceerd en ervaart dit niet als een bewustwordingsprogramma waarmee deelname aangetoond kan worden.

4. Mijn werklaptop gebruik ik in principe niet voor privédoeleinden.

In hoofdstuk 5 van de Gedragscode voor Ambtenaren, gemeente Oude IJsselstreek 2019, zijn regels opgenomen over het privégebruik van laptops, iPad's en mobiele telefoons. Onder andere is beschreven dat het privégebruik van deze elektronische apparatuur in beperkte mate is toegestaan (privémail controleren mag, maar online shoppen of een film streamen niet).

Een groot deel van de respondenten (82,6%) past deze regel meestal of altijd toe. Daaruit blijkt dat deze regel goed bekend is en grotendeels ook goed wordt toegepast. Voor het deel van de respondenten die deze regel niet of soms toepassen wordt de volgende motivatie gegeven:

- Men heeft geen privé laptop en maakt daarom gebruik van de werklaptop.
- Men volgt een (deels) werkgerelateerde studie.
- De werklaptop wordt beschouwd als een bijkomende arbeidsvoorziening die ook privé gebruikt mag worden.
- Zolang men buiten Citrix om werkt is privégebruik veilig en toegestaan volgens een aantal respondenten.

5. Ik vergrendel mijn scherm als ik mijn werkplek verlaat.

In het beleid Logische toegangsbeveiliging is opgenomen dat *'een onbeheerde werkplek is in een ongecontroleerde omgeving altijd vergrendeld. Dit is de afspraak maar blijft afhankelijk van menselijk handelen.'*

Met het verlaten van de werkplek is er geen sprake meer van een gecontroleerde omgeving door de gebruiker zelf. Hierom dient het scherm altijd vergrendeld te worden bij het verlaten van de werkplek.

Het valt op dat bijna driekwart van de respondenten deze regel meestal (31,3%) of altijd (43,6%) opvolgen. Het bewustzijn over en het toepassen van deze regel is daarmee relatief hoog.

Respondenten die onbekend zijn met deze regel of deze niet of soms toepassen geven hiervoor de volgende verklaring:

- Bij het ophalen van een print, koffie of bij toiletbezoek is het verlaten van de werkplek dusdanig kort dat vergrendeling volgens deze respondenten niet nodig is.
- Een aantal respondenten geeft aan collega's (en zeker kamergenoten) te vertrouwen, waardoor vergrendeling niet nodig is.
- Respondenten gaan ervan uit dat het scherm automatisch vergrendeld na een bepaalde periode van inactiviteit.
- Een aantal respondenten minimaliseert openstaande programma's zodat enkel het bureaublad zichtbaar is.
- Een aantal respondenten zet de monitor uit en zijn ervan overtuigd daarmee schermvergrendeling toe te passen.
- Schermvergrendeling wordt door een aantal respondenten als omslachtig ervaren.

6. Ik zorg dat op mijn werkplek geen gevoelige/vertrouwelijke informatie ligt als ik mijn werkplek verlaat.

In zowel het informatiebeveiligingsbeleid, de gedragscode, de Notitie uitgangspunten werkplek en werkruimten en het document Werkafspraken Gemeente Oude IJsselstreek, zijn regels opgenomen met betrekking tot het bewust en veilig omgaan met gevoelige en vertrouwelijke informatie, clear desk-beleid (het opruimen van gevoelige/vertrouwelijke informatie bij het (tijdelijk) verlaten van de werkplek) en het gebruik van lockers en afgesloten opbergruimtes voor dit soort informatie.

Een zeer groot deel van de respondenten (85,6%) is zich bewust van deze gedragsregel en gedraagt zich hier ook meestal of altijd naar. Het relatief kleine deel van de respondenten dat zich niet bewust is van deze regel of zich hier soms naar gedraagt, geeft hierover het volgende aan:

- Bij het ophalen van een print, koffie of bij toiletbezoek is het verlaten van de werkplek dusdanig kort dat het opruimen van deze informatie volgens deze respondenten niet nodig is.
- Een aantal respondenten geeft aan collega's (en zeker kamergenoten) te vertrouwen, waardoor opruimen niet nodig is.
- Een aantal respondenten legt vertrouwelijke/gevoelige informatie op de kop of onder andere niet gevoelige informatie bij het tijdelijk verlaten van de werkplek.
- Het tijdelijk opruimen van gevoelige/vertrouwelijke informatie wordt door een aantal respondenten als omslachtig ervaren.

7. Ik zorg ervoor dat anderen mijn vertrouwelijke / gevoelige gesprekken niet mee kunnen luisteren (zowel op kantoor, thuis als in het openbaar).

In het informatiebeveiligingsbeleid is onder meer benoemd dat '*persoonsgegevens worden beschermd en op een correcte wijze verwerkt zodat de beschikbaarheid, integriteit en vertrouwelijkheid geborgd blijft.'* Daarnaast is opgenomen dat iedere medewerker (zowel tijdelijk als vast, intern of extern) gegevens onder meer beschermt tegen ongeautoriseerde toegang, openbaring, verlies en/of overdracht.

In de gedragscode wordt hier extra aandacht aan besteed en in het document Werkafspraken gemeente Oude IJsselstreek staat specifiek dat *'Belcellen worden gebruikt voor het voeren van een telefoongesprek of een (kort) teamsoverleg'.*

Net als bij regel 5 en 6 valt op dat een heel groot deel van de respondenten zich bewust is van deze regel en zich hier meestal aan houdt (85,2%). Tevens valt positief op dat geen enkel respondenten deze regel ooit gehoord heeft maar vergeten was. De respondenten die deze regel niet kennen of maar soms toepassen geven hiervoor de volgende verklaring:

- Er wordt gewerkt met flexplekken waardoor er te weinig privacy is om telefoon gesprekken alleen te houden.
- Er zijn te weinig beschikbare belcellen en (af te sluiten) spreekkamers om een vertrouwelijk gesprek te kunnen voeren.
- Een aantal respondenten werkt in een ruimte met collega's die hetzelfde werk uitvoeren waardoor gesprekken volgens respondenten meegeluisterd mogen worden.
- Bij sommige vertrouwelijke gesprekken is ook het dossier op de laptop nodig. Men blijft dan op de werkplek bellen.

8. Grote bestanden verstuur ik veilig met Bastion365.

In het Beleid veilig mailen en grote bestanden uitwisselen met Bastion365, is opgenomen dat bestanden groter dan 20mb veilig verstuurt moeten worden via het MyBastion365 portaal en dat dit niet langer via Outlook mogelijk is. In het beleid cryptografie staat daarnaast: *'Om vertrouwelijke en geheime informatie te beschermen is het niet toegestaan om dit type informatie te delen via voorzieningen als webmail, als ook sociale netwerken en clouddiensten (Dropbox, Gmail, etcetera.). Dit vanwege het lage beschermingsniveau, veelal alleen naam en wachtwoord, en het ontbreken van versleuteling.'*

Uit de enquête blijkt dat bijna één derde van de respondenten (30,3%) aangeeft dat deze regel op hen niet van toepassing is. Dit is deels te verklaren omdat men geen grote bestanden hoeft te versturen vanuit de eigen werkzaamheden. 41,5% van de respondenten past deze regel meestal of altijd toe. Bijna één derde van de respondenten (28,2%) geeft aan onbekend te zijn met deze regel, deze te vergeten of soms toe te passen. Verklaringen die hiervoor gegeven worden zijn:

- Men gebruikt liever WeTransfer of DropBox omdat dit makkelijker is voor de ontvangende partij door het ontbreken van 2FA.
- Men ervaart Bastion365 als complex en daarmee niet gebruiksvriendelijk.
- Men is niet op de hoogte dat het mogelijk is om via Bastion365 veilig grote bestanden te versturen.
- De omvang van een bestand zegt niet altijd iets over de vertrouwelijkheid/gevoeligheid van het bestand. Een aantal respondenten maakt een eigen risicoinschatting hiervan en versturen het bestand vervolgens via Dropbox of een andere verzendoplossing.

9. In e-mailberichten open ik geen onbekende url's of bijlagen. Ik vul geen gegevens in bij een (onverwacht) bericht met onbekende afzender.

In de diverse e-Learnings voor nieuwe medewerkers over informatiebeveiliging wordt specifiek aandacht besteed aan het herkennen van en omgaan met verdachte e-mails. Uit de enquête blijkt dat respondenten zich hier goed bewust van zijn en (bijna) altijd naar handelen (95,4%).

Door de 9 respondenten die hebben aangegeven deze regel niet te kennen, deze soms toe te passen of die aangegeven hebben dat deze regel niet op hen van toepassing is, is geen toelichting gegeven.

10. Ik maak geen gebruik van openbare Wifi-netwerken (toegang tot Wifi zonder wachtwoord).

In het informatiebeveiligingsbeleid is opgenomen dat iedere medewerker (zowel tijdelijk als vast, intern of extern) gegevens onder meer beschermt tegen ongeautoriseerde toegang, verandering openbaring, vernietiging, verlies en/of overdracht.

In de gedragscode is daarnaast in hoofdstuk 9 over vertrouwelijke informatie opgenomen dat zorgvuldigheid geboden is bij het geven van toegang tot de computer op de werkplek (of waar je dan ook zit met een iPad of laptop). Aanvullend is in de e-Learnings aandacht besteed aan de werkwijze van internetcriminelen en de risico's van ene openbaar Wifi-netwerk.

Ruim driekwart van de respondenten (78%) past deze regel meestal of altijd toe. De overige respondenten geven verschillende verklaringen voor het niet (kunnen) toepassen van deze regel:

- Het beveiligde Wifi-netwerk is niet altijd even stabiel en daardoor niet werkbaar.
- In sommige gevallen is er geen ander alternatief dan een onbeveiligd Wifi-netwerk.
- Een aantal respondenten wordt niet toegelaten tot het beveiligde Wifi-netwerk (Govroam) en gebruikt daarom het openbare gastennetwerk.
- In het openbaar vervoer maken respondenten voor het werk gebruik van het openbare Wifi-netwerk van de OV-aanbieder.

Tips en suggesties van respondenten

In de enquête is aan respondenten gevraagd of ze nog tips of suggesties hebben om de informatiebeveiliging en privacy te verbeteren. 102 respondenten hebben hierbij iets ingevuld. Samengevat geeft dit het volgende beeld:

- Er is een sterke behoefte aan meer aandacht/bewustwording voor informatiebeveiliging en privacy bij team- en afdelingsvergaderingen. Communicatie over dit onderwerp is momenteel vooral via het intranet en dat leeft minder. Er is behoefte om het gesprek over deze onderwerpen te voeren. Enerzijds zodat men beter begrijpt wat er verwacht wordt, anderzijds om te leren van elkaar.
- Bij veel regels is het 'waarom?' niet gecommuniceerd en welke risico's een regel wegneemt. Door dat beter te communiceren ontstaat er meer draagvlak in het toepassen van de regels.
- Bij nieuwe activiteiten en taken mag informatiebeveiliging en privacy beter geborgd worden.
- De techniek mag verbeterd worden. Genoemd worden het strakker inregelen van de spamfilters, het verbeteren van de Wifi en het verbeteren van Bastion365.
- Er is behoefte aan meer plekken waar privacygevoelige / vertrouwelijke gesprekken gevoerd kunnen worden (zowel in het gemeentehuis als in de DRU waar STOER werkt). Een aantal respondenten geeft aan dat bestaande ruimtes gesplitst zouden kunnen worden.
- Het gebruik van een wachtwoordmanager stimuleren/verplicht stellen.
- Om gebruikers scherp te houden vindt men het wenselijk om de phishing-mails en andere campagnes regelmatig uit te blijven voeren.
- Er mag meer geïnvesteerd worden in een aanspreekcultuur vanuit het oogpunt van verbetering; hou elkaar scherp op de afgesproken informatiebeveiligings- en privacyregels.
- Er is behoefte aan een meer laagdrempelige manier om zaken te melden. Bijvoorbeeld spam direct vanuit Outlook of een incident/datalek zonder dat een zaak aangemaakt moet worden.
- Verbeter de beveiliging van het raadsinformatiesysteem (RIS) door 2FA toe te passen.
- Geef informatiebeveiliging en privacy nog meer een gezicht. Niet alleen via de CISO en de FG, maar vooral ook op management en bestuursniveau.
- Raadsleden hebben behoefte aan inzicht in de regels en specifiek het gebruik van Bastion365.

3. De Techniek

Naast de mens is er de 'harde' kant van informatiebeveiliging en privacy: het geheel van technische maatregelen dat getroffen is om 1) ongeautoriseerde toegang tot de digitale omgeving van de gemeente te voorkomen, en 2) te voorkomen dat data en informatie ongewenst van binnen naar buiten gaat.

Hiervoor heeft onderzoeksbureau NFIR drie verschillende testen uitgevoerd.

- Een penetratietest op de externe infrastructuur.
- Een penetratietest op de interne infrastructuur.
- Een penetratietest op het beveiligde WiFi-netwerk.

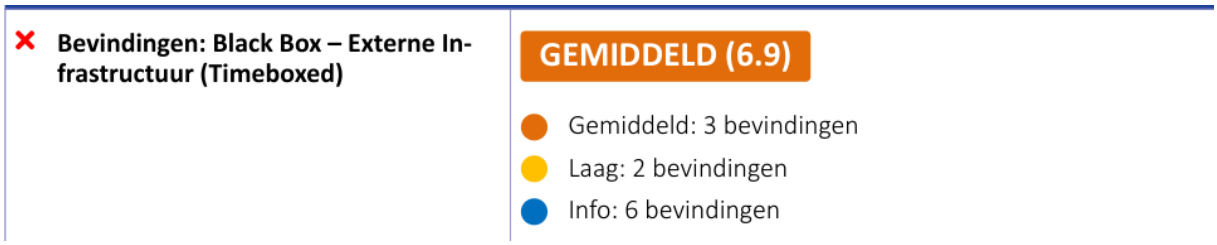
Een toelichting op deze drie onderzoeksmethodieken is beschreven in bijlage 2.

Omdat dit rekenkamerrapport openbaar is worden de geconstateerde bevindingen niet in detail beschreven. De geconstateerde bevindingen bevatten immers vertrouwelijke en bedrijfskritieke informatie, die bij bekendmaking misbruikt kunnen worden. De gedetailleerde resultaten zijn wel gedeeld met de relevante functionarissen in de ambtelijke organisatie. Geconstateerde kritieke bevindingen zijn tijdens het onderzoek direct gemeld en opgelost.

Een beknopte uitwerking van de resultaten volgt hieronder.

3.1 Penetratietest op de externe infrastructuur

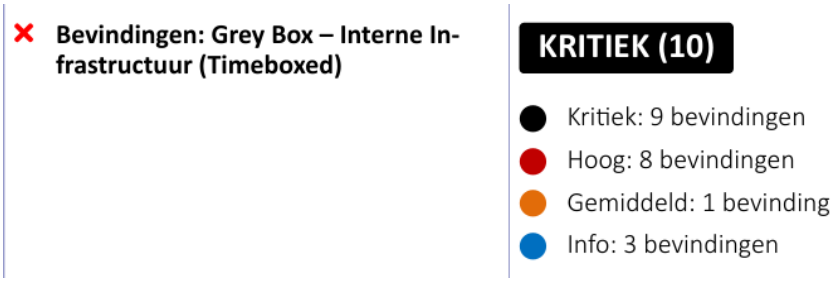
Deze test heeft 11 bevindingen opgeleverd in de volgende categorieën:



De geconstateerde bevindingen richten zich generaliserend op het versterken van de externe beveiliging. Dit zit met name in het toepassen en actualiseren van bepaalde beveiligingsprotocollen op de website en het actualiseren van verlopen certificaten.

3.2 Penetratietest op de interne infrastructuur

Deze test heeft 21 bevindingen opgeleverd in de volgende categorieën:



Zes (6) van de 9 kritieke bevindingen scoren tussen 9,5 en de 10 (waarbij 10 de hoogste score is). Dit betekent dat een hogere score op kritiek niveau niet mogelijk is, wat de ernst van deze bevindingen aangeeft.

De niet kritieke bevindingen constateren dat er medewerkers zijn die gebruik maken van onveilige wachtwoorden en dat het wachtwoordbeleid technisch niet wordt afgedwongen. Daarnaast is geconstateerd dat er diverse gebruikers zijn die meer rechten hebben of toegang hebben tot domeinen dan vanuit hun functie toegestaan is.

3.3 Penetratietest op het beveiligde Wifi-netwerk

Deze test heeft 3 bevindingen opgeleverd in de volgende categorieën:

✖ **Bevindingen: Grey Box – Locatiebe-zoek WIFI (Timeboxed)**	**KRITIEK (9.3)** ● Kritiek: 1 bevinding ● Hoog: 2 bevindingen

Hoewel de kritieke en hoge bevindingen inmiddels zijn opgelost, zijn deze dusdanig gevoelig dat deze niet toegelicht kunnen worden in dit openbare rapport.

4. De Organisatie

Om inzicht te krijgen in de organisatie van informatiebeveiliging en privacy is een dossieronderzoek uitgevoerd. Hierbij zijn de landelijk vastgestelde normenkaders voor informatiebeveiliging (BIO) en privacy (AVG Borgingsproduct 3.0) als toetsingskader gebruikt om de volwassenheid van de organisatie van de informatiebeveiliging en privacy binnen de gemeente vast te stellen.

Het dossieronderzoek is aangevuld met 9 interviews met diverse functionarissen uit de gemeente en de ICT-samenwerking. Een lijst met geïnterviewde personen is opgenomen in bijlage 5.

In het vervolg van dit hoofdstuk worden eerst de belangrijkste bevindingen met betrekking tot de toets op de normenkaders beschreven. Daarna worden zowel voor informatiebeveiliging als privacy de bevindingen, in relatie tot het normenkader en de testen op de Techniek en de Mens, op basis van de interviews beschreven.

4.1 Toets normenkaders informatiebeveiliging en privacy

Er zijn landelijke normenkaders opgesteld voor (gemeentelijke) overheden op het gebied van informatiebeveiliging en privacy. Op het gebied van informatiebeveiliging is dit de BIO. Op het gebied van privacy is dit het AVG-borgingsproduct 3.0. In dit hoofdstuk worden de belangrijkste constateringen beschreven die aangetroffen zijn in de gemeente Oude IJsselstreek aan de hand van een toets op deze normenkaders.

De NIS2 is door het Europees Parlement vastgesteld in januari 2023. Vanaf dat moment is een periode van 21 maanden gestart waarbinnen nationale overheden de NIS2 richtlijn vertaald moeten hebben naar nationale wetgeving. In Nederland wordt dit de Informatiebeveiligingswet. De Informatiebeveiligingswet treedt naar alle waarschijnlijkheid in Q2 2025 in werking en vanaf dat moment dient de gemeente Oude IJsselstreek hieraan te voldoen. De informatiebeveiligingswet is daarom nu al vertaalt in de BIO 2.0, die vanaf Q2 2025 geen richtlijn meer is maar een wettelijke verplichting.

Voor dit rekenkameronderzoek is de situatie in de gemeente Oude IJsselstreek getoetst aan de BIO 2.0 zodat inzichtelijk wordt waar nog werkzaamheden verricht moeten worden om per Q2 2025 te voldoen aan de BIO 2.0.

Toets Baseline Informatiebeveiliging Overheden 2.0 (BIO 2.0)

De BIO 2.0 bestaat uit 203 beheersmaatregelen om te kunnen voldoen aan de actuele eisen op het gebied van informatiebeveiliging. Op basis van het uitgevoerde dossieronderzoek en de afgenomen interviews worden de beheersmaatregelen bij de gemeente Oude IJsselstreek als volgt gescoord:

Status	Aantal
Voldoet geheel (volledig geïmplementeerd)	118
Voldoet deels (gedeeltelijk geïmplementeerd)	51
Voldoet niet (niet geïmplementeerd of niet juist geïmplementeerd)	34
Totaal	**203**

Het is hierbij belangrijk om te weten dat de 203 beheersmaatregelen uit de BIO 2.0 gegroepeerd zijn in thema's. Een thema heeft daarbij een aantal beheersmaatregelen. In een aantal gevallen is het zo dat binnen één thema de meeste beheersmaatregelen dezelfde score hebben gekregen. Dit betekent daarmee ook dat het invulling geven aan een thema waar nu nog 'voldoet niet' op gescoord wordt, direct bij een aantal beheersmaatregelen leidt tot een andere status.

Per status zijn er, overall gezien, de volgende belangrijkste bevindingen:

Voldoet geheel

- Alle benodigde taken, bevoegdheden en verantwoordelijkheden zijn beschreven (o.a. in een compleet en logisch opgesteld mandaatregister) en ingevuld en gebaseerd op de BIO 2.0, AVG en andere relevante wetgeving. De governance is daarmee op orde.
- De CISO en FG hebben, waar nodig, rechtstreekse toegang tot het centraal MT (CMT) en het College. Ze adviseren gevraagd en ongevraagd en er wordt serieus naar geluisterd door besluitvormers. Het CMT en het College maken vervolgens altijd een afweging tussen

gebruiksvriendelijkheid en veiligheid. Hoewel de CISO op papier niet onafhankelijk is gepositioneerd (omdat deze als lijnfunctie en niet als staffunctie rechtstreeks onder de gemeentesecretaris is geplaatst), wordt deze onafhankelijkheid door de CISO wel ervaren.
- Er wordt veel geïnvesteerd in bewustwording, opleiding en training via verschillende vormen (e-Learning, nieuwsberichten, testen, zeepkistbijeenkomsten, afdelings- en teamvergaderingen). Uit de interviews en uit de enquête blijkt ook dat dit grotendeels effect heeft op de medewerkers; hoewel niet alle medewerkers en met name de externen onbekend zijn met de e-Learning, hebben veel medewerkers wel een veiligheidsbewustzijn ontwikkeld door de andere middelen en ontstaat er steeds sterker een (veilige) aanspreekcultuur.
- De omgang met persoonsgegevens in de praktijk gebeurt, op basis van de uitgevoerde steekproef, zeer zorgvuldig. Gegevens worden goed beschermd, papieren aantekeningen worden weggegooid in de beveiligde papierbak en in teamoverleggen wordt altijd een geanonimiseerde situatie i.p.v. een cliënt besproken.
- Er zijn diverse technische toepassingen ingeregeld voor het faciliteren van de informatiebeveiliging en privacy (o.a. veilige mailoplossing, monitoring en respons op het netwerk, malware-detectie, 2-factorauthenticatie, wachtwoordmanager, gescheiden softwareomgevingen).
- De procedure voor het melden en afhandelen van informatiebeveiligingsincidenten en datalekken is compleet beschreven en wordt ook conform uitgevoerd. De procedure is bekend bij gebruikers. Elk incident wat een datalek blijkt wordt gemeld bij de Autoriteit Persoonsgegevens (AP) en bij betrokkenen. Desondanks valt op dat het aantal meldingen in verhouding tot de omvang van de organisatie laag is. Dit komt ook overeen met de resultaten uit de enquête, waarbij medewerkers aangeven niet altijd te weten wat en hoe ze moeten melden.
- Door de gemeente uitgegeven werkplekapparatuur is goed beveiligd tegen ongeautoriseerde toegang (o.a. toepassing van versleuteling (encryptie)).
- Werkplekapparatuur en applicaties worden technisch en functioneel up-to-date gehouden (lifecycle-management wordt toegepast).
- Het back-up en herstelbeleid is actueel en wordt ook conform toegepast en regelmatig getest.
- Het proces van in-, door- en uitstroom van personeel is zodanig ingericht, dat medewerkers bij de start in hun functie bijna altijd beschikken over de juiste rollen en rechten en apparatuur en dat bij uitdienst autorisaties snel worden ingetrokken.

Voldoet deels

- Er zijn veel verplichte beleidsstukken opgesteld maar deze missen soms door de BIO 2.0 verplicht gestelde componenten. Bijvoorbeeld de frequentie van en de wijze waarop het informatiebeveiligingsbeleid wordt geëvalueerd.
- Ongeveer 80% van de volgens de BIO 2.0 benodigde beleidsdocumenten zijn opgesteld en ook geïmplementeerd in de organisatie.
- Diverse onderdelen van het informatiebeveiligingsbeleid zijn in de praktijk niet belegd en/of ingevuld. Zo dienen informatiebeveiliging en privacy onderdeel te zijn van elk projectplan/voorbereiding bij aanschaf of aanpassing van systemen of processen waarbij niet openbare informatie is betrokken. Ook dienen volgens het informatiebeveiligingsbeleid kritieke bedrijfsprocessen onderbouwd bepaald en beschermd te zijn. Omdat een bedrijfscontinuïteitsplan ontbreekt is hieraan (nog) geen invulling gegeven.
- Er zijn op operationeel en gedeeltelijk op tactisch niveau geen formele proceseigenaren in de organisatie op het gebied van informatiebeveiliging- en privacy wat volgens het eigen beleid wel zou moeten. Door het ontbreken van proceseigenaren is momenteel onduidelijk wie formeel een besluit mag nemen over de afhandeling van een melding / mogelijk datalek. Op dit moment verloopt alles via de CISO en de FG, wat niet conform het beleid is.
- Er is geen formeel vastgesteld screeningsbeleid bij de aanname van nieuwe medewerkers en het overleggen van een VOG is alleen bij een aantal specifieke functies verplicht.
- Enkel de verplichte jaarlijkse ENSIA audit wordt uitgevoerd. Interne audits op specifieke onderwerpen, processen en/of afdelingen/teams worden niet uitgevoerd. Door het ontbreken van een goed ingerichte PDCA-cyclus kan hierdoor niet tussentijds (op basis van vastgestelde (potentiële) risico's) gemonitord worden of informatiebeveiliging en privacy goed geborgd zijn.
- In de gedragscode, arbeidsovereenkomst/inhuurovereenkomst of bij de eed/gelofte is niets vastgelegd over de rechten en plichten van een medewerker op het moment dat deze de

organisatie verlaat (bijvoorbeeld dat opgedane kennis en informatie niet gedeeld mag worden).
- Er is geen beleid op het gebied van logging en monitoring. Logging en monitoring wordt wel gedaan door leveranciers van applicaties, maar door het ontbreken van beleid is het onduidelijk of deze logging en monitoring voldoet aan de vereisten van de gemeenten en die van de BIO 2.0.

Voldoet niet

- Er is (nog) geen vastgesteld functieprofiel voor de functie CISO.
- In projecten wordt informatiebeveiliging en privacy niet standaard meegenomen. Er zijn geen formats voor projectplannen om deze thema's structureel te adresseren.
- De in gebruik zijnde softwaresystemen zijn niet geclassificeerd op Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV-classificatie). Hierdoor is niet inzichtelijk welke beveiligingsmaatregelen per softwaresysteem getroffen moeten worden volgens de BIV-classificatie.
- In overeenkomsten van personeel niet in loondienst is geen clausule opgenomen dat deze medewerkers zich dienen te houden aan het informatiebeveiligingsbeleid en de bijbehorende regels.
- Niet bij alle applicaties wordt een (periodieke) controle uitgevoerd op toegangsrechten; hierdoor is niet inzichtelijk of ten alle tijden de juiste personen met de juiste rechten toegang hebben tot de juiste applicaties.
- Er missen een aantal verplichte beleidsstukken zoals een beleid dataclassificatie en een beleid fysieke toegangsbeveiliging.
- In het inkoopbeleid en in leverancierscontracten zijn geen standaard eisen/clausules op het gebied van informatiebeveiliging opgenomen. De Algemene Inkoopvoorwaarden Achterhoekse Gemeenten 2017 (AIAG 2017) en de verwerkersovereenkomsten, bieden onvoldoende houvast om informatiebeveiliging en privacy bij inkoopovereenkomsten te borgen.
- Er is geen meerjarige strategische visie op informatievoorziening en informatiebeveiliging, waardoor niet gepland kan worden op deze thema's. Ook in het informatiebeveiligingsbeleid ontbreekt een heldere visie en ambitie; de huidige visie en ambitie zijn niet meerjarig beschreven.
- Er worden geen formele leveranciersbeoordelingen uitgevoerd op basis van vastgestelde Kritische Prestatie Indicatoren (KPI's). Hierdoor kan de kwaliteit van leveranciers, conform het vastgestelde kwaliteitsniveau, niet gemeten worden. Daarnaast ontbreekt het ook aan contractmanagers om (kritische) contracten goed te managen. Hierdoor ontstaat er een differentiatie in aanpak, frequentie en kwaliteit.
- Er is geen bedrijfscontinuïteitsplan. Hierdoor is onduidelijk welke risico's er gedefinieerd zijn per proces/applicatie en welke risicoscore en risicobehandeling hieraan gekoppeld zijn.
- Er is geen ISMS ingericht op basis van een PDCA-proces. Er is wel een verkenning naar ISMS software opgestart.

Toets AVG Borgingsproduct 3.0

De FG vult zelf al jaarlijks het AVG-borgingsproduct 3.0 in waardoor inzichtelijk is waar nog verbeterpunten zitten op het gebied van het voldoen aan de AVG. Deze wordt ingevuld op basis van een risicoanalyse, aan de hand waarvan maatregelen worden geprioriteerd. De 155 beheersmaatregelen zijn als volgt gescoord:

Status	Aantal
Voldoet (bijna) volledig	107
Voldoet in een kwart tot de helft van de gevallen	17
Voldoet niet of bijna nooit	27
Niet van toepassing	4
Totaal	**155**

Aan 107 van de 155 beheersmaatregelen uit het AVG-borgingsproduct voldoet de gemeente Oude IJsselstreek (bijna) volledig. Dit zit met name op beleid, borging van de taken, bevoegdheden en verantwoordelijkheden (de governance) en het ingeregeld hebben van processen voor burgers (dossierinzage, recht op wijziging, recht op vergeten).

Bij 17 van de 155 beheersmaatregelen wordt hier bij een kwart tot de helft van de gevallen aan voldaan. Dit zijn met name de intern gerichte en meer administratieve werkzaamheden. Hieronder vallen het uitvoeren van DPIA's, het actueel houden van het verwerkingsregister en het hebben van een compleet en actueel overzicht van alle werkprocessen in de organisatie.

Bij 27 van de 155 beheersmaatregelen wordt nog niet of bijna nooit voldaan aan het gestelde. Dit zijn overall gezien de laag-risico beheersmaatregelen zoals het opstellen van procedures voor het uitvoeren van bepaalde werkzaamheden, het actief betrekken van de FG bij het opleiden en trainen van medewerkers en het actueel en volledig houden van alle relevante AVG-informatie met betrekking tot informatiesystemen.

4 van de 155 beheersmaatregelen zijn niet van toepassing, omdat deze beheersmaatregelen gaan over het overhevelen van data naar andere landen. Daar is geen sprake van.

4.2 Aanvullende bevindingen uit de interviews

Als onderdeel van dit rekenkameronderzoek zijn 17 respondenten gesproken (zie bijlage 5B). De input uit de interviews is al deels verwerkt in voorliggende hoofdstukken. In deze paragraaf worden nog een aantal opvallende punten beschreven:

- De gemeente Oude IJsselstreek hanteert een pragmatische aanpak en werkt 'vanuit de bedoeling'. Hierdoor worden soms risico's geaccepteerd die de CISO en de FG niet altijd wenselijk vinden. Een voorbeeld is de keuze om alle, bij de ICT Samen, aangesloten organisaties via één Microsoft omgeving te bedienen in plaats van één omgeving per aangesloten organisatie. De huidige inrichting is technisch en functioneel gemakkelijk en uniform te beheren. Vanuit beveiligings- en privacy-perspectief is dit echter niet wenselijk; een incident bij de ene organisatie kan hierdoor makkelijk doorvloeien naar een andere organisatie binnen de ICT Samen. De technische test uitgevoerd door het NFIR heeft dit ook aangetoond.

- De thema's informatiebeveiliging en privacy worden structureler in de gemeenteraad geagendeerd, via onder andere de auditcommissie. De leden van de auditcommissie bevragen ook actief op deze onderwerpen. De gemeenteraad heeft het thema informatiebeveiliging en privacy geprioriteerd. De betrokkenheid van de gemeenteraad breed bij deze onderwerpen kan nog wel verder verhoogd worden. Met name de bewustwording dat alle gegevens belangrijk zijn en niet alleen de kritieke dossiers.

- De verhouding tot en samenwerking met ICT Samen wordt, door direct betrokkenen bij deze samenwerking, als lastig ervaren. Er is nog regelmatig discussie over wat ICT Samen is; een gastheerschap of een samenwerkingsverband. De gemeente beschouwt ICT Samen als een samenwerkingsverband. In de praktijk gedraagt ICT Samen zich vaak als een gastheerschap die feedback niet altijd kan waarderen. Er zijn een SLA en DVO gesloten maar hier wordt vooral financieel en technisch op gemonitord. Een monitoring en evaluatie van de samenwerking en of deze nog passend is bij de huidige situatie en gezamenlijke en organisatiespecifieke risico's vindt (nog) niet plaats.

  De huidige governance bestaat uit een overlegorgaan waar de gemeentesecretaris aan deelneemt en die vooral financieel stuurt en besluiten neemt over de toetreding van nieuwe leden. Daarnaast is er een ICT-A overleg waar de teamleider I&A aan deelneemt. Dit orgaan neemt besluiten over de (inrichting van de) diensten die ICT Samen levert.
  In de huidige governance zijn geen schriftelijke afspraken gemaakt over wie strategisch, tactisch en operationeel verantwoordelijk zijn bij incidenten en hoe en door wie financiële consequenties van incidenten worden gedragen.

  Er ontbreekt nog een crisisplan en een bedrijfscontinuïteitsplan voor ICT-samen; hierdoor zijn (prospectieve) risico's en te nemen maatregelen indien risico's optreden niet beschreven.

  Er ontbreekt nog een heldere toekomstgerichte governance voor ICT Samen. Informatiebeveiliging en privacy zijn nog niet structureel geborgd binnen ICT Samen op besluitvormingsniveau. Onder geïnterviewden bestaat een sterke wens om afspraken te maken over wie verantwoordelijk is voor de risico-inschatting, beleidsbepaling, risico-acceptatie, verantwoordelijke bij incidenten en de eventuele (financiële) consequenties.

- Diverse organisatieonderdelen zien kansen voor en hebben behoefte aan innovatieve oplossingen op het gebied van AI. Tot op heden wordt door (team)managers aangegeven dat het gebruik van AI niet is toegestaan, zolang er nog geen organisatiebreed beleid voor is. Respondenten verwachten van het Centraal MT een organisatiebreed beleid en toepassingskader voor het verantwoord gebruik van AI.

- De gemeente is 'organisatorisch' aangesloten bij DatalabGO. Er liggen geen (directe) technische verbindingen/koppelingen. DatalabGO maakt hoofdzakelijk gebruik van publieke/openbare data. De gemeente levert bij DatalabGO nog geen gemeentelijke data aan en daar liggen ook nog geen concrete plannen voor.
  DatalabGO maakt via diens gastheer (Gemeente Bronckhorst) wel gebruik van de diensten van ICT Samen en daarmee ook van de dezelfde IT-infrastructuur als de gemeente.

  Er is nog geen visie op datagedreven werken opgesteld. Vooruitlopend op de visie worden vanuit het team I&A voorbereidingen getroffen op het realiseren van een Datawarehouse. Hierbij is de 'architectuur' die is ontwikkeld in overleg met DatalabGO en andere gemeenten(Aalten, Bronckhorst en Doetinchem) die ook daarbij én bij de ICT Samenwerking zijn aangesloten leidend. Het doel hiervan is kennisdeling en om in de toekomst eventueel eenvoudiger te kunnen samenwerken omdat gebruik gemaakt wordt van dezelfde techniek die op eenzelfde wijze is ingericht. Dit blijven wel gescheiden omgevingen; voor de eigen gemeentelijke data wordt géén gebruik gemaakt van het Datawarahouse van DatalabGO.

- De organisatie is zich goed en op tijd aan het voorbereiden op aankomende wet- en regelgeving zoals de Europese NIS 2 richtlijn en de Nederlandse vertaling daarvan in de Informatiebeveiligingswet. Zo zijn het College, de auditcommissie en het CMT door de CISO bijgepraat over dit onderwerp, welke stappen er nog te zetten zijn en is de prioritering van deze stappen vastgesteld.

5. Conclusies

In dit rekenkameronderzoek is de volgende centrale onderzoeksvraag gedefinieerd:

Is de informatiebeveiliging en privacybescherming van de gemeente Oude IJsselstreek – mede in relatie tot samenwerkingsverbanden – doeltreffend en doelmatig ingericht?

Op basis van het uitgevoerde onderzoek kan daar het volgende antwoord op worden gegeven:

De gemeente Oude IJsselstreek heeft haar informatiebeveiliging nog niet op een toekomstbestendige wijze ingericht. Er mist nog een meerjarenvisie op informatiebeveiliging. Daarnaast ontbreekt een toekomstgerichte governance met betrekking tot ICT Samen en zijn risico's in veel gevallen nog onvoldoende inzichtelijk. Beleidsstukken die vastgesteld zijn worden niet (volledig) in de praktijk toegepast. De doelmatigheid en doeltreffendheid van de informatiebeveiliging zijn hierom beperkt.

De gemeente Oude IJsselstreek heeft privacybescherming wel toekomstbestendig, en daarmee doeltreffend en doelmatig, geborgd op strategisch, tactisch en operationeel niveau.

De centrale onderzoeksvraag is uitgewerkt in deelvragen. Deze worden hieronder beantwoordt:

1. Heeft de gemeente op een adequate manier invulling gegeven aan haar informatiebeveiligings- en privacybeleid?

De gemeente Oude IJsselstreek heeft haar privacybeleid opgesteld conform de landelijke kaders (AVG) en deze vertaalt in processen en procedures op tactisch en operationeel niveau. Er is een PDCA-cyclus ingericht en jaarlijks wordt het AVG-borgingsproduct door de Functionaris Gegevensbescherming ingevuld. Op basis hiervan worden actiepunten gedefinieerd voor het komende jaar en vastgesteld door het College.

Voor het thema informatiebeveiliging is er een informatiebeveiligingsbeleid opgesteld en uitgewerkt in diverse (verplichte) aanvullende beleidsstukken op tactisch niveau. De toepassing van het informatiebeveiligingsbeleid is echter beperkt. Met name het daadwerkelijk toepassen van de beschreven governance gebeurt beperkt; zo zijn er strategische taken voor de eenheidsmanagers en teammanagers in het beleid vastgesteld, die bij hen niet bekend zijn en derhalve niet worden uitgevoerd.

2. In hoeverre is de sturing van de gemeente binnen samenwerkingsverbanden toereikend op het gebied van informatiebeveiliging en privacy?

De rekenkamer heeft zich vanaf de start van het onderzoek gericht op ICT Samen. De gemeente Oude IJsselstreek kan beperkt sturen op informatiebeveiliging en privacy binnen ICT Samen.

Er is geen heldere toekomstgerichte governance beschreven voor ICT Samen. Informatiebeveiliging en privacy zijn nog niet structureel geborgd binnen ICT Samen op besluitvormingsniveau. Onder geïnterviewden bestaat een sterke wens om afspraken te maken over wie verantwoordelijk is voor de risico-inschatting, beleidsbepaling, risico-acceptatie, verantwoordelijke bij incidenten en de eventuele (financiële) consequenties.

De CISO en FG worden op dit moment niet proactief betrokken bij advisering over de besluitvorming over onderwerpen die spelen binnen ICT Samen en daarmee alle deelnemers aangaan. De gemeentesecretaris heeft wel periodiek afstemming binnen ICT Samen maar daar wordt voornamelijk gesproken over financiën en de toetreding van potentiële nieuwe deelnemers.

3. In hoeverre zijn risico's en beheersmaatregelen (intern en binnen samenwerkingsverbanden) in kaart gebracht en op welke wijze worden deze consequent opgevolgd?

Intern zijn risico's en beheersmaatregelen gedeeltelijk in kaart gebracht. Vooral op het gebied 'De Mens' wordt hier gestructureerd op gestuurd en gemonitord. Daarentegen zijn een aantal basismaatregelen vanuit de BIO (nog) niet ingeregeld. Zo zijn de in gebruik zijnde

softwaresystemen niet geclassificeerd op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Hierdoor is niet inzichtelijk welke beveiligingsmaatregelen per softwaresysteem getroffen moeten worden volgens de BIV-classificatie. Daarnaast ontbreekt een formeel ingericht ISMS op basis van een ingericht PDCA-proces. Hierdoor is het niet mogelijk op gestructureerd de informatiebeveiliging te monitoren (en daarmee (proactief) risico's vast te stellen en hierop te acteren). Tevens worden leveranciers niet periodiek getoetst middels leveranciersbeoordelingen; hierdoor is niet structureel inzichtelijk of leveranciers zich aan de afspraken houden en daarmee nog geschikt zijn om dienstverlening te leveren.

Op het gebied van 'De techniek' blijkt uit het onderzoek dat er kritieke gaten in de informatiebeveiliging aanwezig waren. Hoewel deze inmiddels gedicht zijn, blijkt hieruit dat de gemeente en ICT Samen onbekend waren met deze risico's.

Binnen ICT Samen en binnen de gemeente OIJ ontbreekt nog een crisisplan en een bedrijfscontinuïteitsplan. Hierdoor zijn (prospectieve) risico's en te nemen maatregelen indien risico's optreden niet beschreven. Indien zich nu incidenten voordoen wordt gehandeld naar eer en geweten op basis van op dat moment geldende inzichten.

4. Op welke wijze anticipeert de gemeente op toekomstige ontwikkelingen (die invloed hebben) op het gebied van informatiebeveiliging en privacy?

Waar het (toekomstige) wettelijke verplichtingen betreft (zoals de NIS2) anticipeert de gemeente Oude IJsselstreek proactief op toekomstige ontwikkelingen. De CISO heeft dit onderwerp proactief opgepakt en besproken met het Centraal MT, het College en in de auditcommissie van de gemeenteraad. Er ligt een concreet actieplan om tijdig te voldoen aan de verplichtingen van de NIS2.

Waar het geen wettelijke verplichtingen betreft, maar wel ontwikkelingen die invloed hebben op informatiebeveiliging en privacy neemt de gemeente Oude IJsselstreek een afwachtende houding aan. Zo is er nog geen AI-beleid en/of kaders op dit gebied, terwijl medewerkers in de uitvoering hier wel behoefte aan hebben en zelfs concrete kansen zien voor toepassing van deze technologie. Eveneens is er nog geen visie op datagedreven werken opgesteld. De gemeente participeert wel in DataLab Go, maar is hier enkel technisch op aangesloten.

5. Hoe wordt de gemeenteraad betrokken bij de thema's informatiebeveiliging en privacy?

De gemeenteraad wordt actief betrokken bij de thema's informatiebeveiliging en privacy. Beide thema's worden structureler in de gemeenteraad geagendeerd, via onder andere de auditcommissie. De leden van de auditcommissie bevragen ook actief op deze onderwerpen.

De gemeenteraad heeft het thema informatiebeveiliging en privacy geprioriteerd. De betrokkenheid van de gemeenteraad breed bij deze onderwerpen kan nog wel verder verhoogd worden. Met name de bewustwording dat alle gegevens belangrijk zijn en niet alleen de kritieke dossiers. Door in raadsvoorstellen het onderdeel informatiebeveiliging en privacy standaard te beschrijven (zoals ook financiën een standaard onderdeel is) kunnen deze thema's binnen de gemeenteraad structureel geborgd worden.

6. Aanbevelingen

Het uitgevoerde onderzoek naar informatiebeveiliging en privacy leidt tot de volgende aanbevelingen voor de gemeenteraad en het College.

Aanbevelingen aan de gemeenteraad

1. Geef het College de opdracht om samen met andere in ICT Samen samenwerkende partijen concrete bestuurlijke en strategische afspraken te maken. In deze afspraken dient een heldere toekomstgerichte governance vastgelegd te zijn. Hierdoor wordt transparant gemaakt wie verantwoordelijk is voor de risico-inschatting, beleidsbepaling, risico-acceptatie, verantwoordelijke bij incidenten en de eventuele (financiële) consequenties.[2]

2. Neem het onderdeel informatiebeveiliging en privacy standaard op in raadsvoorstellen, waardoor dit bij elk onderwerp standaard getoetst en geborgd is.

Aanbevelingen aan het College

3. Stel een visie op en vast voor het gebruik van Artificial Intelligence (AI) en datagedreven werken en draag deze actief uit. Hiermee krijgt de ambtelijke organisatie duidelijkheid over wat wel en niet toegestaan is en daarmee ook welke mogelijkheden er zijn op het gebied van innovatie. Dit geldt ook voor het niet onderzochte onderwerp van algoritmes.

4. Neem het onderdeel informatiebeveiliging en privacy standaard op in collegevoorstellen, waardoor dit bij elk onderwerp standaard getoetst en geborgd is.

5. Los alle bevindingen uit het uitgevoerde technische onderzoek van het NFIR op en laat een nieuw onderzoek uitvoeren om te toetsen of verbeteringen daadwerkelijk gerealiseerd zijn.

6. Stel een Bedrijfscontinuïteitsplan (BCP) op waarin de organisatorische, technische en maatschappelijke maatregelen beschreven zijn die proactief en reactief getroffen (kunnen) worden bij (informatiebeveiligings)incidenten.

7. Realiseer de nog (gedeeltelijk) ontbrekende onderdelen conform Baseline Informatiebeveiliging Overheden 2.0 (BIO 2.0) en zorg dat monitoring op de BIO 2.0 structureel geborgd wordt middels een Information Security Management System (ISMS) op basis van een ingerichte Plan Do Check Act-cyclus (PDCA-cyclus) (zie hoofdstuk 4 van deze rapportage).

8. Onderzoek de mogelijkheden voor implementatie van de door respondenten (in de uitgevoerde enquête) aangedragen verbeterpunten. Communiceer transparant welke verbeterpunten zijn aangedragen en of en hoe deze opgepakt gaan worden.

[2] Deze aanbeveling geldt ook voor de andere gemeenten die aangesloten zijn bij ICT-Samen. Bij de rekenkameronderzoeken naar dit onderwerp bij de gemeenten Doetinchem en Bronckhorst is deze aanbeveling eerder ook gedaan.

Bijlage 1: Bestuurlijke reactie

Beste leden van de rekenkamer,

Op 13 januari 2025 ontvingen wij uw conceptrapportage “VEILIGHEID VERTROUWD!?”, Rekenkameronderzoek naar Informatiebeveiliging en Privacy. Dit onderzoek hebben we met veel interesse tot ons genomen. In deze brief vindt u onze reactie daarop.

Algemene inleiding

Informatiebeveiliging en privacybescherming vormen samen belangrijke voorwaarden voor onze gemeentelijke organisatie die “werken vanuit de bedoeling” als belangrijk uitgangspunt heeft.

Inwoners, ondernemers en anderen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met hun (persoons-)gegevens omgaat. De digitale wereld ontwikkelt zich razendsnel, en daarmee nemen ook de bedreigingen voor onze dienstverlenging toe. Voeg daar de mondiale ontwikkelingen en verhoudingen en een groter wordende afhankelijkheid van het beschikbaar hebben van informatie aan toe, en het is duidelijk dat informatiebeveiliging en privacybescherming tot de cruciale bedrijfsprocessen van onze gemeente behoren. We zijn dan ook blij met dit onderzoek van de Rekenkamer, dat ons waardevolle handvatten geeft voor een versterkte inzet op onze informatieveiligheid.

In deze brief gaan wij per onderdeel nader in op uw onderzoek en doen we een voorstel voor de praktische invulling van een aantal van uw aanbevelingen. Om een goede afweging te kunnen maken is het belangrijk wat de consequentie van aanbevelingen in tijd en geld zijn. Dat is op voorhand voor ons niet altijd goed te doen, dus we verzoeken u onze reactie in dat licht te bezien.

Onderzoeksvraag en onderzoeksaanpak

De centrale vraag die u met uw onderzoek beantwoordt, betreft of de informatiebeveiliging en privacybescherming van de onze gemeente doeltreffend en doelmatig is ingericht, mede in relatie tot de samenwerkingsverbanden. De vraagstelling voor dit onderzoek is helder beschreven in een hoofdvraag die is uitgewerkt in 5 duidelijke deelvragen, waarbij de aanpak met drie velden (Mens, Techniek en Organisatie) als basis voor dit onderzoek, als waardevol wordt ervaren.

De Mens

In het rapport wordt terecht veel aandacht besteed aan “De Mens”. Terecht, want als het gaat om informatieveiligheid is de mens vaak de zwakste schakel. Wij zijn dan ook van mening dat het grootst beïnvloedbare deel van informatiebeveiliging een bewuste medewerker is. Daarom besteden we veel tijd aan verschillende vormen van bewustzijnsversterking (bijvoorbeeld veilige vrijdag en de spion op je pad game) en blijven we dat de komende jaren verder uitbreiden. Als we dan kijken naar de resultaten zien wij dat het klikken op de link in een phishingmail redelijk laag is, en dat het delen van gegevens ook al laag is. Maar wij willen graag deze percentages nog lager brengen. Hoe meer moeite een aanvaller moet doen om bij ons binnen te komen ten opzichte van een andere organisatie, hoe minder de kans is dat een aanvaller de moeite neemt om ons aan te vallen. Daarbij is de medewerker -zowel in vaste dienst als inhuur als in opdracht- een belangrijke schakel van de beveiliging. Dat onze medewerkers, zowel bewust zijn op mail, bellen als de inlooptest zien wij als positief. Het blijft natuurlijk een momentopname en we zien ook punten voor verbetering, zoals bij STOER in de DRU en training van medewerkers bij telefonische phishing.

De Techniek

We waarderen dat als onderdeel van het onderzoek een externe partij een penetratietest heeft uitgevoerd op onze ICT-Omgeving met het doel kwetsbaarheden te vinden in onze organisatie. Het complexe landschap, waar wij met meerdere gemeentes en partners inzitten, zorgt indirect ook voor bepaalde kwetsbaarheden. De bevindingen zijn met de ICT-Samenwerking gedeeld en zijn of worden opgepakt. Wij gaan in deze brief verder niet in op de technische bevindingen

gezien de gevoelige aard ervan. Wij zijn bereid in besloten setting aanvullende reactie te geven op deze bevindingen en daarover in gesprek te gaan.

De Organisatie

Veel van de punten uit het onderzoek herkent het college vanwege de zelfevaluaties die het jaarlijks uitvoert. In 2025 gaat de organisatie dan ook aan de slag met informatiebeveiliging, dat we in samenhang bezien met informatiebeheer- en gebruik. Hieruit ontstaat nieuw informatieveiligheidsbeleid en daaruit voortvloeiende richtlijnen en procedures. Logging van systemen en het monitoren van beleid zullen daar een belangrijke factor in spelen, evenals inkoop- en leveranciersmanagement en in-, door- en uitstroombeleid. Daarnaast is gestart met een project om met behulp van Topdesk en ITIL processen meer structuur aan te brengen in het dagelijkse werk van I&A en gerelateerde processen. Dit valt en staat bij commitment van het gehele management (als proceseigenaren). In 2025 wordt ook gestart met het implementeren van HR-21, waarbij rollen, taken en verantwoordelijkheden van bijvoorbeeld de CISO opnieuw wordt vastgelegd. En op het centraal managementniveau staat IT governance nadrukkelijk op de agenda.

We vinden het belangrijk om stappen te zetten in het voldoen aan de gestelde eisen uit de BIO2. Het tempo waarin we dit kunnen doen hangt af van de capaciteit die dit vraag. Evident voor ons is dat de organisatie dit er niet zomaar bij doen, dus we zullen hierin tot een prioritering moeten komen of hiervoor zal extra geld beschikbaar moeten komen.

Conclusies

Onderstaand gaan wij allereerst in op de antwoorden op de vijf deelvragen en tenslotte geven wij onze reflectie op uw hoofdconclusie, het antwoord op de centrale onderzoeksvraag.

Deelvraag 1. Heeft de gemeente op een adequate manier invulling gegeven aan haar informatiebeveiligings- en privacybeleid?

Uw antwoord op deze onderzoeksvraag is voor ons niet helemaal helder, maar wij interpreteren uw antwoord dat dit voor privacy adequaat is, maar voor informatieveiligheid nog niet.

We zijn het eens met de conclusie over AVG, wij blijven inzetten op het versterken van privacy in onze organisatie. We begrijpen de kritische noot over het operationeel brengen van beleid en procedures rond informatieveiligheid, waaronder de verantwoordelijkheid van eenheidsmanagers en teamleiders. De ambtelijke organisatie zal, mede met de BIO2 in aantocht, extra aandacht besteden aan de (verplichte) rol van het management en de inrichting van IT controls op organisatieniveau.

Deelvraag 2. In hoeverre is de sturing van de gemeente binnen samenwerkingsverbanden toereikend op het gebied van informatiebeveiliging en privacy?

U geeft aan dat wij als gemeente beperkt kunnen sturen op informatiebeveiliging en privacy binnen ICT samen, maar geeft niet aan of dat in uw ogen toereikend is.

De ICT Samenwerking is nu bijna 20 jaar oud en destijds gestart met een samenwerking tussen gemeente Doetinchem en gemeente Oude IJsselstreek om te zorgen dat bij uitval van 1 van de 2 gemeentes, doorgewerkt kan worden bij de andere gemeente. Sinds die periode is de vorm en de taken van de ICT Samenwerking behoorlijk veranderd. Inmiddels is sprake van meer dan 4000 werkplekken verdeeld over meer dan 15 verschillende organisaties. Ook wordt steeds meer in de “cloud” gewerkt in plaats van op de server in het lokale datacentrum. Daarnaast zien we dat de wereld op het gebied van dreigingen en risico’s in het algemeen veranderen. Het aantal aanvallen per dag is hoog, datalekken gebeuren in de samenwerking bijna dagelijks en ook onze leveranciers hebben regelmatig te maken met kwetsbaarheden die onze omgeving beïnvloeden.

Daar hebben wij zelf vaak geen (directe) invloed op. Oude IJsselstreek heeft meermaals geconstateerd en aangegeven dat de governance in deze samenwerking niet (meer) passend is bij de huidige tijd en is op verschillende manieren bezig om deze te (doen) actualiseren. Daarbij zijn we zeer afhankelijk van de andere gemeenten in de samenwerking. Wij merken dat het verbeteren van de governance een langzaam proces is. Mede hierdoor zijn de risico's voor Oude IJsselstreek groter dan wij wenselijk vinden, onder andere op het gebied van informatieveiligheid en bedrijfscontinuïteit.

Hierbij is het belangrijk op te merken dat de ICT Samenwerking een privaatrechtelijke samenwerking betreft via een dienstverleningsovereenkomst, waarvoor de algemeen directeur verantwoordelijk is. In beginsel ligt de sturing en inrichting dan ook op ambtelijk niveau. Onder leiding van de gemeentesecretaris wordt gewerkt om de governance te verbeteren. Dit is een proces waarin een groot aantal partijen betrokken zijn en niet is dat vanuit onze organisatie eenzijdig bepaald kan worden.

Dus wij zien ook verbetermogelijkheden op het gebied van governance en vragen ons tegelijkertijd af of het normenkader op dit onderdeel voldoende antwoord geeft op de vraag of dit leidt tot toereikende sturing. Het vastleggen van verantwoordelijkheden betekent niet per definitie dat je dan de sturing goed hebt ingericht. Het inrichten van governance, zeker op IT-gebied en zeker in een intergemeentelijke samenwerking, gaat verder dan de punten die u noemt in het normenkader.

Deelvraag 3. In hoeverre zijn risico's en beheersmaatregelen (intern en binnen samenwerkingsverbanden) in kaart gebracht en op welke wijze worden deze consequent opgevolgd?

U concludeert dat risico's en beheersmaatregelen gedeeltelijk in kaart zijn gebracht.

Op het gebied van control en risicomanagement zien wij inderdaad verbetermogelijkheden. Met de doorontwikkeling van de ambtelijke organisatie hebben we gekozen voor een separate Concernstaf waarin diverse functies zijn ondergebracht (o.a. concerncontroller, business controllers, interne beheersing, interne controle, concernjurist, CISO) om de organisatie op dit gebied te ondersteunen. Daarbij vraagt dit ook tijd, een andere cultuur en meer in control zijn gaat niet van het een op andere moment, maar we zien dat we hierin in algemene zin stappen zetten, dat blijkt bijvoorbeeld ook uit de

bevindingen van de accountant. We zijn voornemens dit jaar specifieke aandacht te besteden aan het versterken van de interne beheersing op IT gebied. Daarnaast is bekend dat op het gebied van contract- en leveranciersmanagement versterking noodzakelijk is gezien onze verantwoordelijkheid in en van de keten van leveranciers. Ook leert de casus "Crowdstrike" dat onze ICT-Samenwerking continuïteitsrisico's bevat die wat ons betreft om een andere prioritering vragen. Zoals aangegeven kunnen wij dat niet eenzijdig afdwingen en blijft het een afweging tussen verschillende belangen.

Wij waarderen het dat u heeft geconstateerd dat wij proactief bezig zijn met de toekomstige ontwikkelingen.

Deelvraag 4. Op welke wijze anticipeert de gemeente op toekomstige ontwikkelingen (die invloed hebben) op het gebied van informatiebeveiliging en privacy?

U concludeert dat we op toekomstige wettelijke verplichtingen proactief anticiperen, maar dat we voor niet wettelijke verplichtingen die invloed hebben op informatieveiligheid en beveiliging een afwachtende houding aannemen.

We vinden het fijn te lezen dat u geconcludeerd heeft dat privacybescherming toekomstbestendig is ingericht. Het is voor ons niet duidelijk hoe u tot de conclusie komt dat we voor niet wettelijke verplichtingen een afwachtende houding aannemen, daar herkennen wij ons niet in. Inmiddels hebben wij op moment van schrijven AI-beleid en zijn we bezig hier verdere invulling aan te geven. Daarnaast wordt IT-governance gericht opgepakt.

Deelvraag 5. Hoe wordt de gemeenteraad betrokken bij de thema's informatiebeveiliging en privacy?
U stelt dat de gemeenteraad actief betrokken wordt bij deze thema's en dat ook de leden van de auditcommissie actief bevragen op deze onderwerpen, maar dat de betrokkenheid van de gemeenteraad nog wel kan worden verhoogd.

Met betrekking tot deze conclusie willen we graag in gesprek gaan met de griffie om te kijken hoe wij de raad nog beter kunnen betrekken qua bewustzijn. Wellicht is het waardevol om voor de nieuwe raadsperiode een passend inwerkprogramma (op het gebied van informatieveiligheid en privacy) te creëren voor de raad.

Centrale onderzoeksvraag: Is de informatiebeveiliging en privacybescherming van de gemeente Oude IJsselstreek – mede in relatie tot samenwerkingsverbanden – doeltreffend en doelmatig ingericht?

U concludeert dat wij onze informatiebeveiliging nog niet op een toekomstbestendige wijze hebben ingericht, maar privacybescherming wel.

Als de antwoorden op de deelvragen gelezen worden begrijpen wij niet hoe u tot deze hoofdconclusie bent gekomen. Vooral de term toekomstbestendig vinden wij in deze context niet passend. Als u bedoelt dat we nu nog niet voldoen aan de BIO2, dan klopt dat. Dit heeft echter nog geen verplicht karakter, dus het is ook niet onlogisch dat op het moment van uw onderzoek nog niet overal aan wordt voldaan. Wel ondersteunen wij de conclusie dat een meerjarenvisie ontbreekt evenals een toekomstgerichte governance rond de ICT Samenwerking. Daar zijn en worden stappen op ondernomen. Verder verwijzen wij naar de reactie op de verschillende deelvragen hierboven.

Aanbevelingen

Hierna gaan wij in op de aanbevelingen die u doet aan de gemeenteraad.

Geef het College de opdracht om samen met andere in ICT Samen samenwerkende partijen concrete bestuurlijke en strategische afspraken te maken. In deze afspraken dient een heldere toekomstgerichte governance vastgelegd te zijn. Hierdoor wordt transparant gemaakt wie verantwoordelijk is voor de risico-inschatting, beleidsbepaling, risico-acceptatie, verantwoordelijke bij incidenten en de eventuele (financiële) consequenties.

In een privaatrechtelijke samenwerkingsvorm kan de raad geen opdracht geven aan het college. Dus deze aanbeveling delen wij niet, dit zet de raad op het verkeerde been. Het college begrijpt de aanbeveling om samen met ICT Samen samenwerkende partijen te werken aan concrete afspraken. Daar streven wij ook naar en we zijn afhankelijk van de bereidheid van alle aangesloten gemeentes en andere partijen om andere afspraken te maken. De praktijk leert dat niet elke partner hier op dezelfde manier naar kijkt.

Neem het onderdeel informatiebeveiliging en privacy standaard op in raadsvoorstellen, waardoor dit bij elk onderwerp standaard getoetst en geborgd is.

Het is voor ons onvoldoende duidelijk hoe het opnemen van dit punt bijdraagt aan hogere bewustwording. Zoals we aangeven denken wij juist meer aan andere manieren om de raad te betrekken op dit onderwerp. Zouden we al iets dergelijks opnemen in raads- en collegevoorstellen, dan zouden we dit breder willen trekken door het te hebben over belangrijke risico's en getroffen beheersingsmaatregelen, ook op andere gebieden dan alleen informatieveiligheid en privacy. In de praktijk echter gaat dat niet werken. Beheersingsmaatregelen op gebied van informatieveiligheid nemen we bijvoorbeeld op organisatieniveau, door functiescheidingen, gebruik van logische toegangsbeveiligingen of via bepaalde applicatie-controls, dat leent zich niet om in raadsvoorstellen op te nemen. Dat doen we ook niet rond beheersingsmaatregelen op bijvoorbeeld financiële processen waar de accountant over rapporteert. Wij raden deze aanbeveling dan ook af.

Stel een visie op en vast voor het gebruik van Artificial Intelligence (AI) en datagedreven werken en draag deze actief uit. Hiermee krijgt de ambtelijke organisatie duidelijkheid over wat wel en niet toegestaan is en daarmee ook welke mogelijkheden er zijn op het gebied van innovatie. Dit geldt ook voor het niet onderzochte onderwerp van algoritmes.

Een visie op AI en Datagedreven werken ondersteunt het college. Sinds de uitgevoerde deskresearch van de Rekenkamer heeft het college een AI-Strategie vastgesteld en zijn we bezig na te denken over het versterken van datagedreven werken en de inzet van Datalab-GO. We stellen voor om dit advies niet op zichzelf te beschouwen, maar om een brede visie op te stellen voor informatievoorziening en digitale dienstverlening met daaraan verbonden een strategie op governance rond informatievoorziening, ICT en beveiliging. De overlap tussen verschillende beleidsterreinen, zoals bijvoorbeeld ICT, Documentaire informatievoorziening, datagovernance, Inkoop- en leveranciersmanagement, e.d. maakt dat wij meer zien in een overkoepelende visie dan een visie op losse onderwerpen.

Neem het onderdeel informatiebeveiliging en privacy standaard op in collegevoorstellen, waardoor dit bij elk onderwerp standaard getoetst en geborgd is.

Hiervoor verwijzen wij naar punt 2.

Los alle bevindingen uit het uitgevoerde technische onderzoek van het NFIR op en laat een nieuw onderzoek uitvoeren om te toetsen of verbeteringen daadwerkelijk gerealiseerd zijn.

De bevindingen gedaan door NFIR zijn waardevolle bevindingen, wij danken NFIR voor het uitgebreide onderzoek van het netwerk van gemeente Oude IJsselstreek en de ICT-Samenwerking. Adviezen en bevindingen zijn bestudeerd. De opvolging ervan delen wij niet in deze bestuurlijke reactie in verband met het vertrouwelijke karakter van deze bevindingen. Wij zijn bereid in besloten setting aanvullende reactie te geven op deze bevindingen en daarover in gesprek te gaan.

Stel een Bedrijfscontinuïteitsplan (BCP) op waarin de organisatorische, technische en maatschappelijke maatregelen beschreven zijn die proactief en reactief getroffen (kunnen) worden bij (informatiebeveiligings)incidenten.

Het opstellen van een bedrijfscontinuïteitsplan is een punt waarvan wij ook vinden dat we prioriteit aan moeten geven. In 2024 was hiervoor incidenteel budget beschikbaar, door omstandigheden heeft de uitwerking vertraging opgelopen. De verwachting is dat dit uiterlijk eind 2025 opgeleverd wordt inclusief bijbehorende test van de plannen.

Realiseer de nog (gedeeltelijk) ontbrekende onderdelen conform Baseline Informatiebeveiliging Overheden 2.0 (BIO 2.0) en zorg dat monitoring op de BIO 2.0 structureel geborgd wordt middels een Information Security Management System (ISMS) op basis van een ingerichte Plan Do Check Act-cyclus (PDCA-cyclus) (zie hoofdstuk 4 van deze rapportage).

Aanbeveling 7 beschrijft dat de nog ontbrekende onderdelen conform de Baseline Informatiebeveiliging Overheden 2 (BIO2) geïmplementeerd en bijbehorende monitoring structureel geborgd dient te worden. We onderschrijven deze noodzaak, zeker gezien later in 2025 de NIS2/Cbw van kracht wordt waarin staat dat de normen wettelijk verplicht zijn. Toch willen wij de kanttekening plaatsen dat dit punt een behoorlijke belasting zal vormen op de organisatie, zowel in tijd als in middelen. Het Rijk is vooralsnog niet voornemens ons hiervoor financieel te compenseren.

Onderzoek de mogelijkheden voor implementatie van de door respondenten (in de uitgevoerde enquête) aangedragen verbeterpunten. Communiceer transparant welke verbeterpunten zijn aangedragen en of en hoe deze opgepakt gaan worden.

Tijdens het onderzoek is een aantal voorstellen aangedragen als verbeterpunten. Het college is voornemens om alle punten te overwegen, maar constateert dat een aantal punten niet realistisch is om te implementeren ofwel vraagt een andere aanpak dan voorgesteld. Wij denken bijvoorbeeld dat op een aantal plekken bewustzijn een belangrijkere factor is om

kennisachterstand weg te werken dan om "omwegen" te implementeren. We zijn voornemens uiterlijk in Q2 een terugkoppeling te geven aan het personeel.

Tot slot

Wij hebben veel waardering voor het feit dat u dit onderzoek grotendeels in eigen beheer heeft uitgevoerd. Onderzoekstechnisch denken we dat er op onderdelen nog ruimte voor verbetering is. Dat neemt niet weg dat we het belang van een veilige en bewuste organisatie als rode draad zien in dit onderzoek richting het nieuwe normenkader (de BIO2).

We vinden het fijn te lezen dat u geconcludeerd heeft dat privacybescherming toekomstbestendig is ingericht. En we erkennen dat we huiswerk hebben op het gebied van informatieveiligheid en privacy binnen de gehele organisatie en met de ICT-Samenwerking. De verscherpte wet- en regelgeving en parallel het op orde brengen naar het basisniveau van de BIO2, vraagt prioriteit op alle gebieden binnen de bedrijfsvoering in de gemeentelijke organisatie. Investeringen daarin ziet men niet direct terug in betere dienstverlening maar op langere termijn brengt dit wel meer grip, (kosten-)efficiënte en risicobeperking met zich mee, los van het feit dat dit een wettelijke plicht wordt.

Hierbij merken we op dat de huidige en komende periode veel van ons vraagt en dat het essentieel is om te prioriteren. Dit betekent dat als we méér doen op het ene gebied, er minder kan op andere, of dat we meer budget en capaciteit nodig hebben. Het is daarom essentieel dat we als raad, college en ambtelijke organisatie goed met elkaar in gesprek blijven en wederzijdse verwachtingen en mogelijkheden met elkaar delen om prioriteiten te kunnen stellen.

Wij dank u nogmaals voor uw onderzoek en kijken uit naar uw reactie.

Met vriendelijke groet, Burgemeester en wethouders,

Ron Frerix	Mirjam Maasdam
Gemeentesecretaris	Waarnemend burgemeester

Bijlage 2: Nawoord rekenkamer

Op 12 mei 2025 heeft de rekenkamer de uitgebreide reactie van het College ontvangen, waarvoor wij u hartelijk willen danken. Met belangstelling hebben wij uw reactie gelezen.

Wij zijn blij te lezen dat u onze conclusies grotendeels onderschrijft en de meeste aanbevelingen overneemt. Het valt op dat ons onderzoeksrapport al tot de nodige doorwerking heeft geleid. Op basis van deze doorwerking geeft u een extra toelichting bij met name conclusie 4; sinds het aanbieden van ons onderzoeksrapport heeft u AI-beleid vastgesteld en bent u bezig met het inrichten van de IT-governance.

U geeft aan niet te begrijpen hoe de rekenkamer tot de hoofdconclusie is gekomen en de term ‘toekomstbestendig’ niet passend te vinden. De rekenkamer is van mening dat de hoofdconclusie nog steeds geldt. Weliswaar zijn er inmiddels gedurende de periode van 4 maanden van de bestuurlijke reactie goede stappen gezet, maar op basis van de bevindingen uit het technische onderzoek, waar u om veiligheidsredenen in uw reactie niet op reageert, in combinatie met de ten tijde van het onderzoek bekende feiten is de gestelde hoofdconclusie evident.

Het College geeft aan aanbeveling 2 en 4 (om informatiebeveiliging standaard in raads- en collegevoorstellen te adresseren) niet over te nemen. Ten aanzien van deze aanbevelingen merkt de rekenkamer nadrukkelijk op dat informatiebeveiliging breder is dan enkel ICT. Een minimale toets op of informatiebeveiliging van toepassing is, net als communicatie en financiën, blijft volgens de rekenkamer nodig om informatiebeveiliging en privacy structureel in de organisatie te borgen.

De rekenkamer begrijpt dat het realiseren van de overige aanbevelingen een balans vraagt bij het vinden en inzetten van beschikbare middelen, zeker in financieel moeilijke jaren. Hierom waardeert de rekenkamer het dat het College de urgentie van deze aanbevelingen inziet en hier binnen beschikbaar budget en tijd op in wil zetten.

De rekenkamer dankt u nogmaals voor uw reactie en ziet graag de voortgang op de realisatie van de aanbevelingen terug in de jaarlijks verplichte terugkoppeling aan de gemeenteraad.

Met vriendelijke groet,

Arend Kloosterman

Voorzitter Rekenkamer Oude IJsselstreek

Bijlage 3: Verklarende woordenlijst

Afkorting	Betekenis	Toelichting
2FA	Two Factor Authentication	Het toegang krijgen tot bepaalde informatie en/of systemen via twee identificatiemechanismen. Voorbeelden zijn het gebruiken van een wachtwoord in combinatie met een eenmalige toegangscode ontvangen via de telefoon.
AI	Artificial Intelligence / Artificiële Intelligentie	Een techniek waarbij slimme softwareoplossingen op basis van een gegenereerd taalmodel geautomatiseerd taken uit kunnen voeren (bijvoorbeeld het schrijven van een tekst of het maken van een verslag op basis van een audio-opname).
AVG	Algemene Verordening Gegevensbescherming	De Nederlandse wetgeving op het gebied van privacybescherming.
BIO	Baseline Informatiebeveiliging Overheden	Het door de VNG vastgestelde normenkader voor informatiebeveiliging gebaseerd op de ISO27001
CISO	Chief Information Security Officer	De functionaris die verantwoordelijk is voor het voldoen aan de BIO.
DPIA	Data Protection Impact Assessment	Een manier om een proces, product en/of systeem te toetsen op de risico's voor gegevensbescherming en privacy.
DVO	Dienstverleningsovereenkomst	Een document waarin beschreven staat welke dienstverlening tegen welke voorwaarden Opdrachtnemer levert aan Opdrachtgever.
FG	Functionaris Gegevensbescherming	De functionaris die onafhankelijk toetst of aan de AVG wordt voldaan.
ISMS	Information Security Management System	Een intern ingerichte processystematiek om gestructureerd het voldoen aan de vereisten uit de BIO te borgen.
ISO27001	International Standardization Organisation 27001	De internationale norm voor informatiebeveiliging uitgegeven door ISO.
NIS2	Network and Information Security 2	Een verplichte Europese richtlijn op het gebied van informatiebeveiliging.
PDCA	Plan, Do, Check, Act	Ook wel de Cirkel van Demming genoemd; een systematiek om kwaliteitsprocessen te borgen.
SLA	Service Level Agreement	Een document waarin gegarandeerde serviceniveaus over de kwaliteit van dienstverlening van Opdrachtnemer voor Opdrachtgever zijn beschreven.
url	uniform resource locator	Het internetadres in de browser of waar een koppeling/link naar verwijst.

Bijlage 4: Onderzoeksverantwoording

A) De Mens

Het thema 'De Mens' is op verschillende manieren onderzocht. Het externe onderzoeksbureau NFIR heeft een aantal testen uitgevoerd. De rekenkamer heeft daarnaast zelf een enquête uitgezet. Hieronder volgt een korte toelichting op de onderzoekscomponenten bij het thema 'De Mens'.

Mail phishing

Mail phishing betekent dat via een legitiem uitziende mail getracht wordt om inloggegevens van de mailontvanger te verkrijgen.

Het NFIR heeft voor de mail phishing test alle medewerkers (inclusief inhuur) van de gemeente Oude IJsselstreek, het college en de leden van de gemeenteraad en fractievolgers een mail toegezonden. In deze mail werd de ontvanger erop geattendeerd dat een grote hoeveelheid persoonlijke documenten verwijderd was. Via een inlogknop konden de documenten teruggehaald worden.

Indien de ontvanger inloggegevens (gebruikersnaam en wachtwoord) invulde kwam vervolgens de boodschap in zicht dat dit een test betrof en tevens tips hoe de gebruiker had kunnen herkennen dat het een phishing mail betrof.

Voice phishing

Voice phishing betekent dat een ontvanger gebeld wordt door een legitiem klinkende 'collega' met het doel om inloggegevens van de ontvanger te verkrijgen.

Het NFIR heeft voor de voice phishing geprobeerd 16 medewerkers van de gemeente Oude IJsselstreek te bereiken. Hierbij deed het NFIR zich voor als een medewerker van de ICT servicedesk waarbij de computerinstellingen gecontroleerd moesten worden. Via het helpdeskportal van de ICT-servicedesk werd vervolgens geprobeerd om inloggegevens (gebruikersnaam en wachtwoord) te achterhalen.

Inlooptest

Een inlooptest betekent dat een 'mystery guest' onderzoekt in hoeverre toegang tot beveiligde delen van een pand mogelijk is.

Het NFIR heeft voor de inlooptest het gemeentehuis in Gendringen en STOER in de DRU in Ulft bezocht en (zonder zich te melden bij de receptie) onderzocht hoe ver hij in de beveiligde medewerkersgedeelten van het pand kon komen. Hierbij werd tevens onderzocht in hoeverre vertrouwelijke gegevens (foto's van openstaande beeldschermen, papieren dossiers/aantekeningen) en gemeentelijke/persoonlijke eigendommen (telefoons, sleutels, etc.) buitgemaakt konden worden.

Voor het geval de mystery guest betrapt zou worden had hij een door de gemeentesecretaris getekende vrijwaringsverklaring bij zich.

Enquête gedragsregels

Bij de gemeente Oude IJsselstreek zijn diverse gedragsregels op het gebied van informatiebeveiliging en privacy met medewerkers gedeeld.

De rekenkamer heeft middels een enquête onder alle medewerkers, het college en raadsleden onderzocht in hoeverre de gedragsregels bekend zijn en opgevolgd worden. Tevens is onderzocht of bepaalde gedragsregels als nuttig worden ervaren of dat er juist gedragsregels missen.

De volledige blanco enquête is opgenomen in bijlage 4.

B) De Techniek

Het thema 'De Techniek' is volledig onderzocht door onderzoeksbureau NFIR. Hiervoor zijn drie verschillende onderdelen onderzocht:

- Een penetratietest op de externe infrastructuur. Hiermee wordt onderzocht of het mogelijk is om als buitenstaander in te breken op het netwerk van de gemeente. Er wordt getest of de buitendeuren goed op slot zitten.
  De test is uitgevoerd zonder voorinformatie vanuit / over de organisatie; een zogeheten black-box penetratietest. Hiermee werd een zo realistisch mogelijk scenario getest, als ware het een echte internetcrimineel toegang probeert te krijgen tot het netwerk van de gemeente.

- Een penetratietest op de interne infrastructuur. Hiermee wordt onderzocht hoever de onderzoeker zich door het netwerk (bijvoorbeeld toegang tot afdelingsapplicaties en documenten) kan bewegen nadat externe toegang is verkregen. Er wordt getest of de binnendeuren goed op slot zetten en of er gescheiden zones (segmentering) zijn toegepast. De test is uitgevoerd met bepaalde voorinformatie vanuit / over de organisatie; een zogeheten grey-box penetratietest. Dit is bewust gedaan om te voorkomen dat de omgeving van andere deelnemers van de ICT-samenwerking betrokken zouden worden bij de test.

- Een penetratietest op het beveiligde WiFi-netwerk. Hiermee wordt onderzocht of het mogelijk is om in te breken op het beveiligde WiFi-netwerk en zo toegang te verkrijgen tot het interne netwerk en/of apparaten die gebruik maken van dit beveiligde WiFi-netwerk.

Bij de testen heeft het NFIR gebruik gemaakt van diverse internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden, te weten:

- Penetration Testing Execution Standard (PTES): standaard ten behoeve van infrastructuur penetratietesten.
- CWE(CommonWeaknessEnumeration):Lijst van veelvoorkomende softwarefouten voor het verbeteren van softwarebeveiliging.
- CommonVulnerability Scoring System (CVSS): wordt gebruikt om de ernst van de kwetsbaarheden te classificeren

C) De Organisatie

Om inzicht te krijgen in de organisatie van informatiebeveiliging en privacy is een dossieronderzoek uitgevoerd. Hierbij zijn de landelijk vastgestelde normenkaders voor informatiebeveiliging (BIO) en privacy (AVG Borgingsproduct 3.0) als toetsingskader gebruikt om de volwassenheid van de organisatie van de informatiebeveiliging en privacy binnen de gemeente vast te stellen.

Het dossieronderzoek is aangevuld met 9 interviews met diverse functionarissen uit de gemeente en de ICT-samenwerking. Een lijst met geïnterviewde personen is opgenomen in bijlage 3

D) Normenkader

Voor de beantwoording van de onderzoeksvragen is het volgende normenkader gehanteerd:

Onderzoeksvragen	Normen
1. Heeft de gemeente op een adequate manier invulling gegeven aan haar informatiebeveiligings- en privacybeleid?	- Door het college is informatiebeveligings- en privacybeleid vastgesteld en dit wordt actief uitgedragen. - Jaarlijks worden interne en externe factoren die van invloed (kunnen) zijn op informatiebeveiliging en privacy meegenomen in jaarplannen. - Informatiebeveiliging en privacy zijn kwalitatief en kwantitatief geborgd in

	benodigde functies en rollen. - Medewerkers zijn en blijven op de hoogte van de regels omtrent informatiebeveiliging en privacy en handelen hier ook naar. - Het informatiebeveilgings- en privacybeleid is vertaald in benodigde deel-beleidsstukken en (interne) richtlijnen. - Er wordt periodiek gerapporteerd aan het management over de status van informatiebeveiliging en privacy.
2. In hoeverre is de sturing van de gemeente binnen samenwerkingsverbanden toereikend op het gebied van informatiebeveiliging- en privacy?	- De gemeente heeft inzichtelijk met welke partijen informatie en data gedeeld worden en heeft hiervoor de benodigde maatregelen getroffen zoals verwerkersovereenkomst en registratie in een verwerkingsregister. - Partners en leveranciers rapporteren jaarlijks over de stand van zaken op het gebied van informatiebeveiliging en privacy. - Bij samenwerkingsverbanden waar sprake is van gedeelde ICT-voorzieningen is formeel beschreven wie, waarvoor verantwoordelijk is en in de praktijk conform ingericht.
3. In hoeverre zijn risico's en beheersmaatregelen (intern en binnen samenwerkingsverbanden) in kaart gebracht en op welke wijze worden deze consequent opgevolgd?	- Het normenkader BIO en het AVG Borgingsproduct 3.0 worden structureel gehanteerd om sturing te geven. - Jaarlijks wordt een risicoanalyse uitgevoerd en vastgesteld, op basis waarvan door de gemeente maatregelen worden getroffen. - Informatie en data zijn goed beschermd tegen ongewenste invloeden van zowel buitenaf als van binnenuit. - Er zijn procedures vastgesteld hoe om te gaan met informatiebeveiligings- en privacyincidenten en/of datalekken en er wordt conform gehandeld. - Informatiebeveiliging- en privacy zijn in de praktijk ingericht conform de PDCA-cyclus. - Op alle systemen waarin informatie en data verwerkt wordt is logging en monitoring geïmplementeerd.
4. Op welke wijze anticipeert de gemeente op toekomstige ontwikkelingen (die invloed hebben) op het gebied van informatiebeveiliging en privacy?	- Informatiebeveiliging en privacy zijn gebaseerd op het principe van 'de lerende organisatie'. - Relevante Wet- en regelgeving wordt tijdig herkend en vertaald naar de lokale praktijk. - Er wordt geanticipeerd op technologische en maatschappelijke ontwikkelingen die invloed (kunnen) hebben op het toepassen van

		informatiebeveiligings- en privacybeleid, door kansen en risico's vast te stellen en beleid en jaarplannen hierop in te richten.
5.	Hoe wordt de gemeenteraad betrokken bij de thema's informatiebeveiliging en privacy?	- Over het functioneren van informatiebeveiliging en privacy wordt jaarlijks gerapporteerd aan de raad middels de ENSIA[3]. - In geval van datalekken die gemeld worden bij de Autoriteit Persoonsgegevens wordt de raad geïnformeerd over de inhoud en de getroffen maatregelen.

E) Transparantieparagraaf

Het onderzoek naar informatiebeveiliging en privacy is door de rekenkamer grotendeels in eigen beheer uitgevoerd. De CISO van de gemeente Oude IJsselstreek heeft ook een nevenfunctie als raadslid bij de gemeente Bronckhorst. De leden van de rekenkamer Oude IJsselstreek zijn ook, als rekenkamerlid of als fractievolger, gelieerd aan de gemeente Bronckhorst.

Hierom is voorafgaand aan de start van het onderzoek een afweging gemaakt naar mogelijke belangenverstrengeling en/of integriteitsconflicten. Uit deze afweging is naar voren gekomen dat de leden van de rekenkamer Oude IJsselstreek geen conflicterende belangen hebben en dat het onderzoek naar informatiebeveiliging en privacy op een professionele, onafhankelijke en kwalitatief hoogwaardige manier zelfstandig uitgevoerd kan worden. Als extra waarborg heeft de rekenkamer Prae Advies als onafhankelijk adviseur betrokken bij het onderzoek.

[3] ENSIA (Eenduidige Normatiek Single Information Audit) is een initiatief van gemeenten en de ministeries van BZK en SZW. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid.

Bijlage 5: Geraadpleegde bronnen

A) Documenten

Voor het onderzoek zijn de volgende documenten geraadpleegd (in alfabetische volgorde):

- Documentatie ENSIA Cyclus 2022
- Documentatie ENSIA Cyclus 2023
- 01 U-WA.05 - Rapport dataclassificatie eDiensten Burgerzaken v1.7
- 01 U-WA.05 Classificatie informatie GOUW
- 01 U-WA.05 Ordeningsstructuur zaaksysteem
- 02 Voorlopige planning audits
- 03 + 31 Gem. Doetinchem Uitwijk datacenters
- 03 Backup Gem. Doetinchem - DAP v1.0
- 04 Logische Toegangsbeveiliging
- 05 Notitie_Uitgangspunten_werkplek_vastgesteld_CMT_20240404_ V3
- 05 Werkafspraken organisatie vastgesteld door CMT 20240606
- 06 Cryptografie
- 07 20231003 autorisatiemodel
- 08 Shortlist Werkafspraken medewerkers medewerkers intranet 1-6-2019
- 09 Bescherming tegen malware - afhandelen van Microsoft Defender meldingen – Concept
- 10 'Beleid' veilig mailen en grote bestanden uitwisselen met Bastion 365
- 10 Handleiding veilig grote bestanden verzenden met Bastion365 OIJ
- 10 Handreiking voor veilig mailen met Bastion365
- 11 Wijzigingsbeheer
- 12 + 22 + 23 + 38 Informatieveiligheids- en privacybeleid 2022-2026
- 13 Besluit Informatiebeheer gemeente Oude IJsselstreek
- 13 Handboek Vervanging OIJ 2.3 (vastgesteld 22-10-2019)
- 14 20210205 Definitief indelingsadvies CISO
- 15 Aanpak bedrijfscontinuïteitsplan
- 17 Beoordeling (pre)DPIA sjabloon
- 17 DPIA model 092023 sjabloon
- 18 A 1 191022 Model nieuwe arbeidsovereenkomst bepaalde tijd
- 18 A 1.1.1 191022 Model nieuwe arbeidsovereenkomst onbepaalde tijd
- 19 Projectplan template NIEUW
- 20 Standaard Verwerkersovereenkomst
- 21 20191203 Gedragscode
- 24 AIAG2017 actuele versie 2022
- 24 Inkoop- en aanbestedingsbeleid Gemeente Oude IJsselstreek 2017 versie 1-1-2022
- 26 Besluit eed en belofte
- 26 Integriteitsbeleid Ambtenaren 2019
- 27 e-learning informatiebeveiliging nieuwe medewerker week 1
- 27 e-learning informatiebeveiliging nieuwe medewerker week 2
- 27 e-learning informatiebeveiliging nieuwe medewerker week 3
- 27 e-learning informatiebeveiliging nieuwe medewerker week 4
- 28 Besluit ongewenste omgangsvormen gemeente Oude IJsselstreek
- 28 regeling melding vermoeden misstand versie 2014.pdf__ig
- 29 Groslijstensystematiek 2019 gemeente Oude IJsselstreek versie 10-12-2019
- 31 Netwerkoverzicht gemeente Oude IJsselstreek
- 32 - Organisatiegegevens KPN Certificaten
- 32 - Persoonsgebonden certificaten (Gefilterd op status geldig)
- 32 - Servercertificaten (Gefilterd op status geldig)
- 34 Normenkader 2023
- 35 Rekenkamer werkprocessen met persoonsgegevens OIJ - v2
- 36 Personeelshandboek gemeente Oude IJsselstreek
- 37 Borgingsproduct-3.0-Toetsingskader OIJ
- 37 Digitale weerbaarheid AVG gemeente Oude IJsselstreek 2023-1
- 39+ 40 e-learning bewustwording medewerker
- 41 Privacy Statement
- 42 + 43 Procedure Datalekken
- 43 Responsible disclosure
- 45 Bijlage I - Algemene Samenwerkingsvoorwaarden
- 45 Bijlage II - Algemene uitvoeringsvoorwaarden

- 45 Governance ICT Samen
- 47 Inventarisatie VOGP
- 49 Omgaan met tijd
- 49 Regeling arbeidsduur en werktijden def
- 50 202210-Verwerkingsregister-gemeenten-v1.3
- 51 DPIA Kredit - Allegro juni 2024 in uitvoering
- 52 Wachtwoordbeleid
- 53 Plattegrond vlekkenplan 1e verdieping definitief 20240606
- 53 Plattegrond vlekkenplan BG definitief 20240606
- Formulier Aanvraag users-account
- Formulier inhuur
- Formulier Integriteitsverklaring
- Mandaatregeling 2024
- OIJ visie op dienstverlening 12-3 def
- Overeenkomst van Opdracht bureau
- Overeenkomst van Opdracht ZZP
- Persoonsgegevens inhuur
- Visie op informatie definitief
- Memo_Incident Crowdstrike
- Plattegronden Gemeentehuis

Aanvullend zijn de volgende rapportages opgesteld door onderzoeksbureau NFIR en verwerkt in het voorliggende rekenkamerrapport:

- 24156 - Bazzano - Management Samenvatting – 20241007
- 24156 - Bazzano - Rapportage – 20241007
- 24156 - Bazzano - Rapportage phishing simulatie v1.0
- 24156 - Bazzano - Voice Phishing 20241018
- 24156 - Bazzano Mystery guest rapportage 20241018

B) Interviews en praktijkcasussen

Voor het rekenkameronderzoek zijn de volgende functionarissen geïnterviewd (in alfabetische volgorde):

Naam	Functie
Andre Putker	Eenheidsmanager Fysieke Ontwikkeling
Angelique Dhondt	Kwaliteitsmedewerker Wmo en Jeugd
Anne Marie Nas	Functionaris Gegevensbescherming (FG)
Arjan Vaartjes	Teamleider informatisering & Automatisering
Bram Grob	Coördinator infrastructuur en applicaties (ICT Samen)
Bob Konings	Eenheidsmanager Publiekszaken, Economie en Maatschappij
Dennis Ankersmid	Adviseur vergunningen
Frank Weghaus	Teamleider ruimtelijke ordening
Iety Hendriks	Teamleider Personeel & Organisatie
Jacques Roosendaal	Inkoopcoördinator
Linda Tackenkamp	Eenheidsmanager Sociaal Domein
Maartje Nijman	Teamleider Wmo en Jeugd
Mirjam Maasdam	Waarnemend burgemeester
Robbert van Velsen	Chief Information Security Officer (CISO)
Ron Frerix	Gemeentesecretaris
Sarah Peprah	Adviseur vergunningen APV en Bijzondere wetten
Yvon Didden	Teamleider Economie en Maatschappij

Bijlage 6: Uitgezette enquête

Welkomstpagina

Beste raadsleden, collegeleden en medewerkers van de gemeente Oude IJsselstreek,
De rekenkamer is een onderzoek gestart naar informatiebeveiliging en privacy. Omdat jij als lid van de raad, het college of als medewerker dagelijks met (persoons)gegevens of andere vertrouwelijke informatie werkt, heb ook jij een rol in informatieveilig werken.

Jouw collega's van informatiebeveiliging en privacy hebben een aantal gedragsregels opgesteld die jou helpen om bewust met informatiebeveiliging en privacy om te gaan. Met 4 vragen wil de rekenkamer toetsen in hoeverre door raadsleden, collegeleden en medewerkers van de gemeente Oude IJsselstreek informatieveilig en privacybewust gehandeld wordt. Ook willen we achterhalen of bepaalde gedragsregels wel of niet als nuttig worden ervaren.

Het invullen van de vragenlijst neemt maximaal 5 minuten van je tijd in beslag. Uiteraard is het invullen volledig anoniem.

Alvast bedankt voor je bijdrage aan dit onderzoek.

Met vriendelijke groet,

Rekenkamer Oude IJsselstreek

Vraag 1: In hoeverre houdt je je aan de onderstaande gedragsregels op het gebied van informatiebeveiliging en privacy?

Hieronder zijn de belangrijkste regels weergegeven op het gebied van informatiebeveiliging en privacy. We vragen je om per regel aan te geven in hoeverre je je hieraan houdt. Hierbij is er geen goed of fout. Het helpt om meer inzicht te krijgen in de effectiviteit van de regels en om hier van te leren als organisatie. Het is daarom belangrijk om het onderstaande eerlijk in te vullen vanuit je eigen beleving.

	Is dit een gedragsregel?	Oei, die was ik vergeten; ik moet daar beter op gaan letten	Ik pas deze regel soms toe	Ik pas deze regel meestal toe	Dit doe ik altijd!	Deze regel is op mijn werkzaamheden niet van toepassing
1. Een informatiebeveiligings- en/of privacy-incident meld ik via het beschikbare meldformulier **(Verplicht)**	O	O	O	O	O	O
2. E-mails met (bijzondere) persoonsgegevens en/of vertrouwelijk/gevoelige data verstuur ik altijd via de beveiligde mailoplossing Bastion365 **(Verplicht)**	O	O	O	O	O	O
3. Ik volg jaarlijks het bewustwordingsprogramma informatiebeveiliging en privacy **(Verplicht)**	O	O	O	O	O	O
4. Mijn werklaptop gebruik ik in principe niet voor privédoeleinden **(Verplicht)**	O	O	O	O	O	O
5. Ik vergrendel mijn	O	O	O	O	O	O

scherm als ik mijn werkplek verlaat **(Verplicht)**						
6. Ik zorg dat op mijn werkplek geen gevoelige/vertrouwelijke informatie ligt als ik mijn werkplek verlaat **(Verplicht)**	O	O	O	O	O	O
7. Ik zorg ervoor dat anderen mijn vertrouwelijke / gevoelige gesprekken niet mee kunnen luisteren (zowel op kantoor, thuis als in het openbaar). **(Verplicht)**	O	O	O	O	O	O
8. Grote bestanden verstuur ik veilig met Bastion365 **(Verplicht)**	O	O	O	O	O	O
9. In e-mailberichten open ik geen onbekende url's of bijlagen. Ik vul geen gegevens in bij een (onverwacht) bericht met onbekende afzender. **(Verplicht)**	O	O	O	O	O	O
10. Ik maak geen gebruik van openbare Wifi-netwerken (toegang tot Wifi zonder wachtwoord) **(Verplicht)**	O	O	O	O	O	O

Vraag 2: Indien je je aan één of meer van bovenstaande regels niet houdt, waarom is dat dan? **(Verplicht)**

Opmerking: Mogelijke redenen kunnen bijvoorbeeld zijn: 'regel nr. 'x' is niet makkelijk toepasbaar' of 'regel nr. 'y' snap ik niet hoe ik die moet toepassen.'

Vraag 3: In je dagelijks werk kom je veel tegen. Heb je tips om de informatiebeveiliging en/of privacy aan te scherpen? **(Verplicht)**

Om de onderzoeksresultaten te kunnen specificeren en bruikbare aanbevelingen te kunnen doen, vragen we om de afdeling aan te vinken waarvoor je werkzaam bent.

Vraag 4: Voor welke afdeling ben je werkzaam? **(Verplicht)**

Opmerking: Afdelingen zijn gesorteerd op alfabetische volgorde

O Bedrijfsvoering
O BUOR
O College van Burgemeester en Wethouders
O Concernstaf
O Fysieke ontwikkeling
O Gemeenteraad
O Griffie
O Publiekszaken, Economie & Maatschappij (PEM)
O Sociaal Domein

Einde van de vragenlijst

Hartelijk dank voor het invullen van de vragenlijst. Hierdoor heb je een waardevolle bijdrage geleverd aan het rekenkameronderzoek én de verdere verbetering van de informatiebeveiligings- en privacyprocessen binnen de gemeente.

De respons op deze vragenlijst wordt onderdeel van het rekenkamerrapport, wat na afronding van het onderzoek en presentatie aan de gemeenteraad beschikbaar komt.

Heb je naar aanleiding van het invullen van deze vragenlijst nog vragen of wil je nog iets kwijt? Neem dan contact op met rekenkamer@oude-ijsselstreek.nl