

Strategisch Informatiebeveiligingsbeleid

2026 - 2029

Vastgesteld door	College van B&W gemeente Texel
Datum vaststelling	[datum collegebesluit]
Geldig tot	31 december 2029
Versie	1.2
Opsteller	R.J. van Vliet, CISO - gemeente Texel
Opvolger van	Strategisch IBB 2020-2023

Versiebeheer

Versie	Datum	Door	Wijziging
1.0	9-6-2026	Robert Jan van Vliet	Definitief gemaakt
1.1	25-6-2026	Daniël Witte	wijziging in wetgevingen
1.2	29-6-2026	Daniël Witte	Afstemming PDCA/jaarplan met bestuurlijk voorstel

Inhoud

1. Inleiding.....	3
1.1 Wat is informatiebeveiliging?	3
2. Ambitie en visie	4
2.1 Visie	4
2.2 Ambitiebeschrijving	4
3. Kaders en standaarden.....	5
4. Reikwijdte (scope)	6
4.1 Wat valt binnen de scope?	6
5. Doelen en uitgangspunten.....	7
5.1 Strategische doelen.....	7
5.2 Uitgangspunten	7
5.3 Randvoorwaarden	8
6. Organisatie, taken en verantwoordelijkheden.....	9
6.1 Three Lines Model.....	9
6.2 Rollen en verantwoordelijkheden	10
7. Controle en verantwoording	12
7.1 PDCA-cyclus.....	12
7.2 ENSIA-verantwoording.....	12
7.3 Audits.....	12
Interne audits	12
Wettelijk verplichte audits	13
7.4 Beleidsherziening	13
Vaststelling.....	14

1. Inleiding

Deze nota beschrijft het Strategisch Informatiebeveiligingsbeleid (IB-beleid) van gemeente Texel voor de jaren 2026-2029. Het vervangt het 'Strategisch Informatiebeveiligingsbeleid 2020-2023'.

Dit beleid is richtinggevend en kaderstellend. Het legt de koers, visie, uitgangspunten en eigenaarschap voor informatiebeveiliging vast. De uitwerking in concrete maatregelen en activiteiten vindt plaats in het IB-jaarplan, dat door het College van B&W wordt vastgesteld.

De basis voor dit beleid zijn de Baseline Informatiebeveiliging Overheid versie 2 (BIO2), de NIS2-richtlijn (Cyberbeveiligingswet), ISO27001 en de 10 bestuurlijke principes voor informatiebeveiliging.

1.1 Wat is informatiebeveiliging?

Informatiebeveiliging draait om het beschermen van drie kernwaarden:

Kernwaarde	Betekenis
Beschikbaarheid	Informatie en systemen zijn beschikbaar wanneer medewerkers, inwoners en partners ze nodig hebben.
Integriteit	Informatie is juist, volledig en niet onbedoeld gewijzigd.
Vertrouwelijkheid	Informatie is alleen toegankelijk voor degenen die daartoe bevoegd zijn.

De bescherming van persoonsgegevens (privacy) valt buiten de scope van dit beleid en wordt afzonderlijk behandeld in het privacybeleid van gemeente Texel. Beide beleidsdocumenten zijn complementair.

2. Ambitie en visie

Ambitie

"Gemeente Texel ontwikkelt zich naar een hoger volwassenheidsniveau waarin informatiebeveiliging geen taak van alleen ICT is, maar een gedeelde verantwoordelijkheid die in alle lagen van de organisatie wordt gevoeld en gedragen. In 2029 is veiligheidsbewustzijn een vast onderdeel van onze cultuur en dagelijkse manier van werken."

2.1 Visie

Informatiebeveiliging is geen technische bijzaak, maar een gedeelde verantwoordelijkheid van de gehele organisatie; van bestuur tot medewerker. Risico's worden vroegtijdig herkend, bewust afgewogen en structureel beheerst. Voorbeeldgedrag van bestuur, management en leidinggevenden is daarin essentieel.

Cyberdreigingen, geopolitieke spanningen, menselijke fouten en afhankelijkheid van (cloud)leveranciers maken het noodzakelijk dat Texel weerbaar en voorbereid is. Informatiebeveiliging wordt integraal meegenomen in alle processen en projecten.

2.2 Ambitiebeschrijving

Voor de gemeente is informatie één van de belangrijkste bedrijfsmiddelen. Toegankelijke en betrouwbare informatie is essentieel voor een goede dienstverlening aan onze inwoners. De algehele ambitie van de gemeente is om zich verder te ontwikkelen als verantwoordelijke, aanspreekbare en servicegerichte organisatie die transparant en proactief verantwoording aflegt aan inwoners, raadsleden en de rijksoverheid. De bescherming van waardevolle informatie staat daarin centraal. Hoe waardevoller de informatie, hoe zwaarder de maatregelen die getroffen moeten worden. Voor informatiebeveiliging betekent dit dat wij stapsgewijs willen groeien van een reactieve naar een aantoonbaar beheerste en proactieve aanpak, waarin maatregelen onderbouwd, herhaalbaar en controleerbaar zijn.

Het is hierbij belangrijk te beseffen dat 100% veiligheid niet bestaat. Zeker als het gaat om cyberdreigingen. Nieuwe technologieën en trends verbeteren enerzijds de dienstverlening, maar brengen anderzijds voortdurend onvoorziene risico's met zich mee, waardoor steeds nieuwe kwetsbaarheden en aanvalsmethoden kunnen ontstaan. Daarnaast speelt de menselijke factor een grote rol. Juist daarom is het vergroten van bewustzijn en het versterken van een veilige werkcultuur een kernonderdeel van onze ambitie. Medewerkers die risico's herkennen, veilig handelen en zich medeverantwoordelijk voelen, vormen de belangrijkste schakel in onze weerbaarheid. Het is, ondanks technische en organisatorische maatregelen, onmogelijk om de risico's tot nul terug te brengen.

Een effectief en goed ingericht risicomanagementproces is daarom randvoorwaardelijk voor het behalen van onze ambitie op het gebied van informatiebeveiliging. Risicomanagement helpt om weloverwogen keuzes te maken en de juiste prioriteiten te stellen om de gemeente veilig te houden. Door risicomanagement steeds beter te verankeren in onze processen en besluitvorming, groeien wij gestaag naar het volwassenheidsniveau dat wij nastreven.

3. Kaders en standaarden

Dit beleid is gebaseerd op de volgende wet- en regelgeving en normen:

Kader / Standaard	Toelichting
Baseline Informatiebeveiliging Overheid 2	Verplicht normenkader voor alle Nederlandse overheden . Gebaseerd op ISO 27001/27002. Schrijft risicogestuurd werken voor.
NEN-EN-ISO/IEC 27001:2023	Internationale norm voor informatiebeveiligingsmanagement. Basis voor inrichting van het ISMS.
NEN-EN-ISO/IEC 27002:2022	Best-practice maatregelen voor informatiebeveiliging.
De aanstaande Cyberbeveiligingswet (Cbw), naar verwachting in werking in 2026	Europese richtlijn, uitgewerkt in Nederlandse wet. Gemeenten zijn essentiële entiteiten met verscherpte eisen en meldplicht.
Dreigingsbeeld IBD (jaarlijks)	Actueel beeld van dreigingen voor Nederlandse gemeenten. Basis voor jaarlijkse beleidsactualisatie.
IBD-ondersteuningsaanbod	Texel sluit aan bij de gezamenlijke aanpak van de IBD: risicoanalyses en maatregelen via de kracht van het collectief.

Naast de bovenstaande kaders en standaarden worden de 10 bestuurlijke principes van de VNG (Vereniging van Nederlandse Gemeenten)/ IBD (Informatiebeveiligingsdienst) gehanteerd. De 10 bestuurlijke principes voor informatiebeveiliging zijn een aanvulling op het normenkader van de Baseline Informatiebeveiliging Overheid (BIO) en gaan over de waarden die bestuurders zichzelf opleggen. Ze richten zich nadrukkelijk op de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie en ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets misgaat met de beveiliging van informatie binnen gemeentelijke processen, kan dit directe gevolgen hebben voor inwoners, ondernemers en partners. Informatiebeveiliging hoort daarom thuis op de bestuurstafel.

De principes zijn:

- Bestuurders bevorderen een veilige cultuur.
- Informatiebeveiliging is van iedereen.
- Informatiebeveiliging is risicomanagement.
- Risicomanagement is onderdeel van de besluitvorming.
- Informatiebeveiliging heeft ook aandacht in (keten)samenwerking.
- Informatiebeveiliging is een proces.
- Informatiebeveiliging kost geld.
- Onzekerheid dient te worden ingecalculeerd.
- Verbetering komt voort uit leren en ervaring.
- Het bestuur controleert en evalueert.

4. Reikwijdte (scope)

4.1 Wat valt binnen de scope?

Dit beleid geldt voor alle informatie, informatiesystemen, processen en medewerkers van gemeente Texel, inclusief bestuur en management, inhuurkrachten, leveranciers en ketenpartners die namens de gemeente informatie verwerken.

Het beperkt zich niet tot ICT: ook fysieke beveiliging (o.a. toegang algemene werkruimten, serverruimte, archief), operationele technologie, gedrag en werkwijze vallen eronder.

5. Doelen en uitgangspunten

5.1 Strategische doelen

Dit beleid richt zich op een aantal hoofddoelen voor de periode 2026-2029:

- Het managen van de informatiebeveiliging
- Adequate bescherming van bedrijfsmiddelen
- Het versterken van veiligheidsbewustzijn en een veilige werkcultuur
- Het adequaat reageren op incidenten
- Het beschermen van (kritieke) bedrijfsprocessen
- Voldoen aan de wettelijke verplichtingen op het vlak van informatiebeveiliging en dit op ieder moment met bewijs kunnen aantonen
- Het waarborgen van de naleving van dit beleid
- Het aantoonbaar verhogen van de volwassenheid van informatiebeveiliging, gemeten aan de hand van BIO2 en ENSIA

5.2 Uitgangspunten

De volgende uitgangspunten zijn bindend voor de hele organisatie:

1. Verantwoordelijkheid in de lijn: Elke afdelingsmanager is verantwoordelijk voor informatiebeveiliging binnen zijn of haar afdeling. Deze verantwoordelijkheid is niet overdraagbaar.
2. Eigenaarschap: Alle processen, systemen en gegevens hebben een eigenaar. De eerste lijn is eigenaar van de processen, systemen, gegevens én risico's binnen het eigen domein. De eigenaar bepaalt de classificatie en is verantwoordelijk voor passende maatregelen.
3. Risicogestuurd werken: Maatregelen worden bepaald op basis van risicobeoordeling, niet op basis van een standaardlijst. Risico's die bewust worden geaccepteerd, worden expliciet vastgelegd.
4. Verankering in de organisatie: Informatiebeveiliging is structureel ingebed in de planning, sturing, coördinatie en verantwoording van de organisatie. Het is geen losstaand traject naast de reguliere bedrijfsvoering, maar een vast onderdeel ervan.
5. Continu verbeteren: Informatiebeveiliging is een continu verbeterproces. Plan-Do-Check-Act vormt het fundament van het IB-managementsysteem.
6. Security by design: Beveiliging wordt vanaf het begin meegenomen in nieuwe projecten, processen en systemen, niet achteraf toegevoegd.
7. Bewust en verantwoord handelen: Medewerkers, inhuurkrachten en leveranciers handelen veilig en zorgvuldig, en melden incidenten of vermoedelijke inbreuken tijdig. Dit beleid geldt voor iedereen die met gemeentelijke informatie werkt; naleving is niet vrijwillig.

8. Beheersing van leveranciers en ketenpartners: Informatiebeveiliging wordt ook geborgd in de samenwerking met leveranciers, ketenpartners en andere externe partijen. Eisen worden contractueel vastgelegd en periodiek getoetst.

5.3 Randvoorwaarden

Voor de uitvoering van dit beleid gelden de volgende randvoorwaarden:

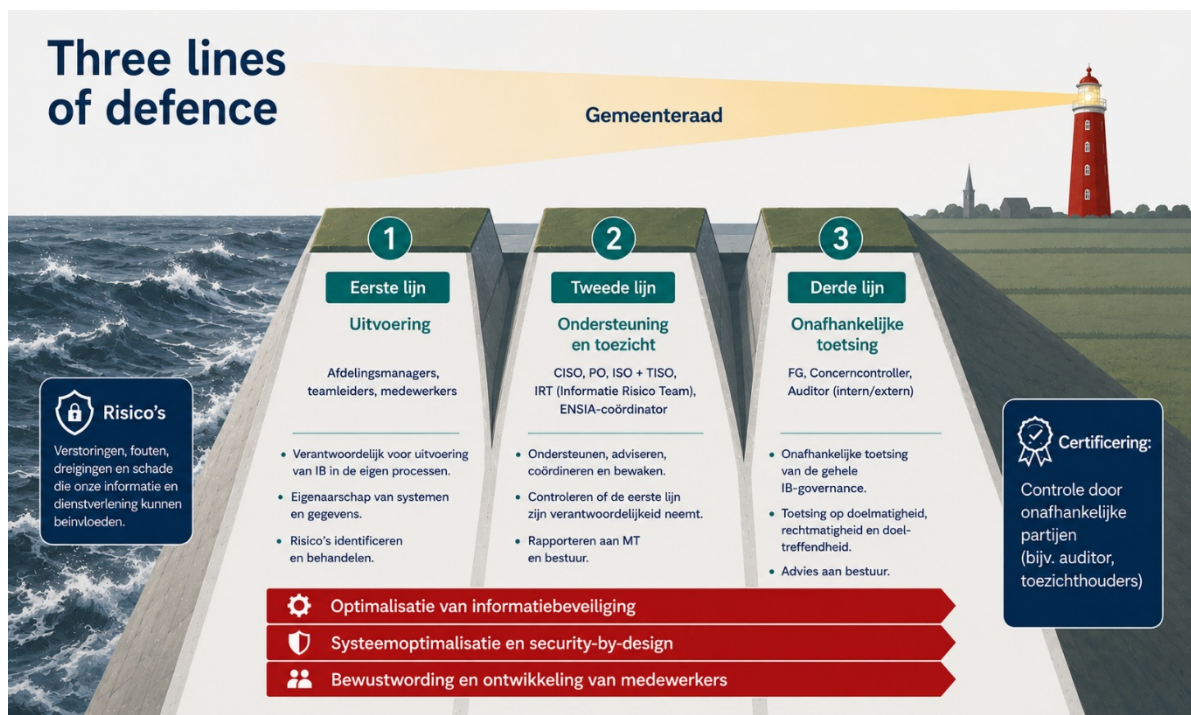
- Eigenaarschap van het beleid: De portefeuillehouder informatiebeveiliging is bestuurlijk eigenaar van dit strategisch beleid. De gemeentesecretaris is ambtelijk verantwoordelijk voor de uitvoering. De CISO is beleidshouder en adviseert beide.
- Jaarplan: Het College van B&W stelt onder haar verantwoordelijkheid jaarlijks het IB-jaarplan vast. Het jaarplan opent met een terugblik op het voorgaande jaar – onder meer de uitkomsten van de management review, ENSIA en audits – en vertaalt de strategische lijn vervolgens naar concrete acties, programma's, investeringen, audits en trainingen. De CISO bereidt het jaarplan voor, op basis van dit beleid, ENSIA-uitkomsten, risicoanalyses, het dreigingsbeeld van de IBD en input van afdelingsmanagers.
- Budget: De begroting voorziet jaarlijks in budget voor uitvoering van het IB-jaarplan.
- Bewustwording en training: Bewustwording en training zijn structurele activiteiten, niet incidenteel. Iedere medewerker volgt periodiek een basistraining; specifieke doelgroepen (ontwikkelaars, beheerders, BOA's, bestuurders) krijgen aanvullende, op de rol toegesneden training.
- Contractuele borging bij externen: Eisen aan informatiebeveiliging worden vastgelegd in contracten met leveranciers, ketenpartners en gemeenschappelijke regelingen, en periodiek getoetst.

6. Organisatie, taken en verantwoordelijkheden

6.1 Three Lines Model

Texel hanteert het Three Lines Model voor de governance van informatiebeveiliging. Dit model maakt helder wie verantwoordelijk is voor uitvoering, wie bewaakt, en wie toetst.

Lijn	Wie	Rol
Eerste lijn	Afdelingsmanagers, teamleiders, medewerkers	Verantwoordelijk voor uitvoering van IB in de eigen processen. Eigenaarschap van systemen en gegevens. Risico's identificeren en behandelen.
Tweede lijn	CISO, PO, ISO + TISO, IRT (Informatie Risico Team), ENSIA-coördinator	Ondersteunen, adviseren, coördineren en bewaken. Controleren of de eerste lijn zijn verantwoordelijkheid neemt. Rapporteren aan MT en bestuur.
Derde lijn	FG, Concerncontroller, Auditor (intern/extern)	Onafhankelijke toetsing van de gehele IB-governance. Toetsing op rechtmatigheid en doeltreffendheid. Advies aan bestuur.



Figuur 1 Three Lines Model

6.2 Rollen en verantwoordelijkheden

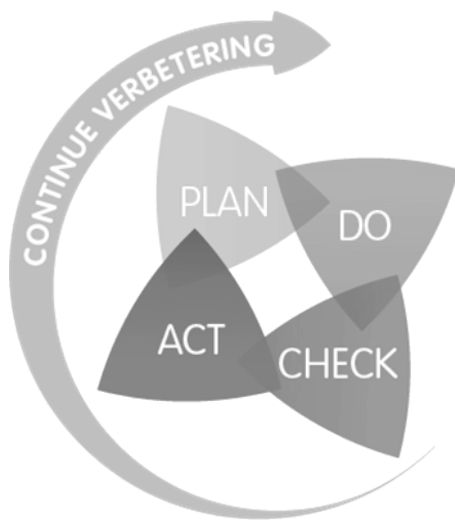
Rol	Verantwoordelijkheid	Concrete verplichtingen
College van B&W	Eindverantwoordelijk voor informatiebeveiliging. Stelt strategisch beleid vast. Stelt mensen en middelen beschikbaar.	Beleid en IB-jaarplan vaststellen. ENSIA In Control Verklaring ondertekenen. Jaarlijkse verantwoording aan Raad.
Portefeuillehouder informatiebeveiliging	Bestuurlijk eigenaar van dit beleid binnen het College. Aanspreekpunt voor de Raad en bij ernstige incidenten.	IB agenderen in College en Raad. Raadsvragen beantwoorden. Bestuurlijke woordvoering bij significante incidenten. Sturen op uitvoering van het IB-jaarplan.
Gemeentesecretaris / Management Team	Risico-eigenaar van organisatiebrede en strategische risico's.	IB als vast agendapunt in P&C-cyclus. Tactisch beleid goedkeuren.
Afdelingsmanagers (1e lijn)	Eigenaar van processen, systemen, gegevens en risico's binnen hun afdeling. Deze verantwoordelijkheid is niet overdraagbaar. Nazien op eisen die worden gesteld aan leveranciers en/of gemeenschappelijke regelingen.	Risicoanalyses uitvoeren. Toezien op uitvoering behandelplan met maatregelen. Medewerkers trainen. Uitdragen van informatiebeveiliging naar de teams. Zorgdragen dat incidenten worden gemeld en opgevolgd. Rapporteren aan College van B&W.
Teamleiders (1e lijn)	Eerste aanspreekpunt voor uitvoering van IB op teamniveau. Werken onder verantwoordelijkheid van de afdelingsmanager.	Toezien op naleving binnen het team. Incidenten signaleren en doorgeleiden naar de CISO. Zorgen dat medewerkers deelnemen aan bewustwordingstrainingen. Zorgen dat er consequent controles plaatsvinden op werkprocessen (bv op autorisaties).
CISO (2e lijn)	Coördineert IB organisatiebreed. Adviseert gevraagd en ongevraagd. Rapporteert onafhankelijk aan MT en College.	IB-jaarplan voorbereiden. Dreigingsbeeld vertalen. Jaarlijkse rapportage aan MT/College. IRT voorzitten.
ISO + TISO (2e lijn)	Ondersteunen de CISO op strategisch en tactisch niveau. Vertalen beleid naar afdelingen.	Tactisch beleid uitwerken. Afdelingen begeleiden bij risicoanalyses. Verbinding CISO en werkvloer.
FG - Functionaris Gegevensbescherming (3e lijn)	Onafhankelijk intern toezicht. Voor informatiebeveiliging relevant waar IB-keuzes gevolgen hebben voor de	Signaleren van IB-tekortkomingen die privacy raken. Adviseren bij datalekken en DPIA's. Onafhankelijk

	verwerking van persoonsgegevens. Werkt op die snijvlakken samen met CISO en het MT.	rapporteren aan het College van B&W.
PO - Privacyofficer (2e lijn)	Werkt samen met de CISO en FG op het snijvlak van informatiebeveiliging en privacy. Brengt de privacy-dimensie in bij IB-keuzes (verwerkersovereenkomsten, nieuwe systemen, dataverwerking).	Toetsen van verwerkersovereenkomsten op IB- en privacy-eisen. Bijdragen aan risicoanalyses bij nieuwe verwerkingen. Coördinatie met FG en CISO.
IRT - Informatie Risico Team (2e lijn)	Actieve multidisciplinaire adviesgroep. Draagt organisatiebrede verantwoordelijkheid.	Inventariseert en beheerst interne risico's. Adviseert het MT. Bewaakt de afgesproken maatregelen.
ENSIA-coördinator (2e lijn)	Coördineert ENSIA-verantwoording.	ENSIA zelfevaluatie coördineren. Rapporteren aan MT en College.
Concerncontroller (3e lijn)	Onafhankelijk toezicht op rechtmatigheid en doelmatigheid van de bedrijfsvoering, waaronder IB. Kan IB-kwesties separaat agenderen bij MT en College.	Toezen op naleving IB-verplichtingen in begroting en jaarrekening. Signaleren bij College indien nodig.
Auditor (3e lijn)	Onafhankelijke toetsing van de IB-governance.	Interne audits uitvoeren. Rapporteren aan MT en College.
Alle medewerkers (1e lijn)	Werken conform dit beleid en geldende procedures.	Veilig omgaan met informatie. Jaarlijkse bewustwordingstraining. Incidenten melden.

7. Controle en verantwoording

7.1 PDCA-cyclus

Informatiebeveiliging wordt gestuurd volgens de PDCA-cyclus. Strategisch beleid, het IB-jaarplan en risicoafwegingen vormen daarbij de basis voor sturing (Plan), de uitvoering ligt in de lijn (Do), monitoring, audits en verantwoording vormen de toetsing (Check), en op basis daarvan worden beleid, maatregelen en prioriteiten bijgesteld (Act). De bijsturing uit de Act-fase wordt verwerkt in het eerstvolgende IB-jaarplan, dat opent met een terugblik op het voorgaande jaar. Zo komen sturing (vooruitblik) en verantwoording (terugblik) in één document samen en stuurt en monitort het College via één jaarlijks moment: de vaststelling van het IB-jaarplan.



Figuur 2 PDCA Cyclus

7.2 ENSIA-verantwoording

De gemeente legt jaarlijks verantwoording af via de ENSIA-systematiek. De ENSIA-coördinator verzamelt informatie bij de afdelingsmanagers. Het College ondertekent de In Control Verklaring (ICV), die als onderdeel van het jaarverslag naar de Gemeenteraad gaat. De ICV dekt informatiebeveiliging, DigiD, SUWI en BRP af.

7.3 Audits

De gemeente kent twee sporen van audits: interne audits ter verificatie van de eigen beheersing, en wettelijk verplichte audits die voortkomen uit specifieke wet- en regelgeving.

Interne audits

- Naast de wettelijk verplichte audits worden jaarlijks interne audits uitgevoerd ter verificatie van de werking van de informatiebeveiligingsmaatregelen. De scope wordt jaarlijks vastgesteld in het IB-jaarplan op basis van risicoanalyse en eerdere bevindingen.
- De CISO rapporteert bevindingen en aanbevelingen aan het MT. Bij significante bevindingen wordt ook de portefeuillehouder geïnformeerd.
- Opvolging van bevindingen wordt vastgelegd en gemonitord; openstaande punten worden meegenomen in de volgende auditcyclus.

Wettelijk verplichte audits

- DigiD- en SUWI-audits worden jaarlijks uitgevoerd door een onafhankelijk extern bureau, conform de wettelijke verplichting. De rapportages worden aangeleverd bij Logius (DigiD) en het Inlichtingenbureau (SUWI).
- De ENSIA-zelfevaluatie wordt jaarlijks uitgevoerd en gedeeltelijk extern geverifieerd (zie §7.2).

7.4 Beleidsherziening

Dit strategisch beleid wordt jaarlijks beoordeeld op actualiteit in een management review. Aanleiding voor herziening zijn in elk geval: wezenlijke wijzigingen in wet- of regelgeving, significante veranderingen in het dreigingslandschap, of majeure organisatiewijzigingen. De uitkomst van de beoordeling wordt als terugblik opgenomen in het eerstvolgende IB-jaarplan en meegenomen in de behandeling van de begroting in Q2.

Vaststelling

Dit Strategisch Informatiebeveiligingsbeleid 2026-2029 is vastgesteld door het College van B&W van gemeente Texel in de vergadering van [datum].

Dit beleid vervangt het 'Strategisch Informatiebeveiligingsbeleid 2020-2023' en treedt in werking op de dag na vaststelling.

De Burgemeester,

De Gemeentesecretaris,
