

Informatiebeleid 2023 - 2026

Visie: Extern & eigen ambities

Wat komt er op Asten af

- Ontwikkelingen**
- Omgevingswet
 - Wet Open Overheid
 - Nieuwe Archiefwet
 - Samenhangende objectregistratie
- Landelijke informatie projecten**
- Landelijke Voorziening Digitaal Stelsel
 - Omgevingswet
 - Baseline Informatiebeveiliging Overheid (BIO)
 - Common Ground
- Lokale projecten 2024**
- Evaluatie overgang naar ICT NML
 - Focus op digitale vaardigheden en informatieveiligheid
 - Doorontwikkeling Informatiemanagement & veiligheid



Goed bestuur

- Coalitieakkoord 2022-2026 "Gedreven door passie en ambitie"
- **Collegiaal:** gelijkwaardig als uitgangspunt, zorgen voor een open en constructief debat;
 - **Transparant en integer:** betrouwbaar, betrokken, duidelijk en met respect naar eenieder;
 - **Midden in de gemeenschap:** inwoners en ondernemers opzoeken;
 - **Met visie, lef en plezier:** 'samen aanpakken en genieten';
 - **Lerend en zelf corrigerend vermogen:** kwetsbaar durven opstellen, regelmatig met elkaar evalueren;
 - **Open communicatie:** laten zien wat de gemeente voor haar inwoners doet en op een passende wijze communiceren.

Ambities Asten

Asten is een sterke, zelfstandige gemeente die actief en intensief samenwerkt.
Waar leggen we de focus:

- Bouwen en goed wonen
- Vitaal buitengebied
- Klimaat, energie en duurzaamheid
- Sterke lokale economie en mobiliteit
- Bruisende en aantrekkelijke kernen
- Sociaal en gezond
- Veiilige buurt en thuis
- Financieel gezond

Ambities dienstverlening

Asten biedt vraaggerichte, goede en snelle dienstverlening.

- Wij zijn voor een zichtbare, toegankelijke en transparante gemeentelijke organisatie.
- Maatschappelijke uitdagingen gaan we samen met andere aan. Wij maken ze concreet in plannen en projecten en brengen ze tot uitvoering.
- Investeren in relaties & krachten bundelen. Wij zien noodzaak en kansen in het versterken van de samenwerking binnen de Peel als gevolg van de grotere maatschappelijke opgaven.

Strategisch/Richten

Informatiehuis

Het informatiehuis bestaat uit verschillende lagen. Deze lagen zijn met elkaar verbonden en hebben invloed op elkaar.

- Organisatie en ketenpartners
- Informatie en data
- Applicaties en beheer
- Infrastructuur ICT NML



Regie op Informatie

Asten heeft de ICT automatisering bij ICT NML ondergebracht, dit betekent dat Asten:

- Hier samen met de andere 5 partners regie over voert.
- Applicatiebeheer zelf organiseert als aanspreekpunt voor ICT NML.
- Portfolio van applicaties afstemt op efficiënt gebruik.
- Zelf een beeld vormt van ontwikkelingen op gebied van het applicatielandschap.
- Informatiemanagement als belangrijke schakel inzet binnen de ambities van de organisatie.

Doel van informatiebeleid

Doel van het informatiebeleid is:

- De ambities vertalen naar de informatievoorziening
- Inzicht te geven in te verwachten ontwikkelingen op gebied van informatievoorziening
- Op basis daarvan handvatten te bieden voor het maken van keuzes en het doen van investeringen
- Integraliteit organiseren tussen gebruik, veiligheid en integriteit
- Begrijpelijk maken van de waarde van informatie



Doel van informatiebeveiligingsbeleid

Doel van informatiebeveiliging is:

- Asten als een aantoonbare betrouwbare partner
- De betrouwbaarheid van de informatievoorziening waarborgen
- In control zijn en hierover verantwoording afleggen
- Geen ongeoorloofd gebruik en/of -toegang tot de informatievoorziening
- Het versterken van de informatieveiligheid door betere afstemming met ketenpartners en andere partijen

Tactisch/Inrichten

Verantwoordelijkheden en bevoegdheden

- Het College is kader stellend als het om informatiebeleid & informatieveiligheid gaat.
- Het MT is integraal eindverantwoordelijk voor het informatiebeheer & informatiebeveiliging.
- De informatiemanager (CIO) is verantwoordelijk voor het opstellen van het informatiebeleid.
- De CISO is namens het College verantwoordelijk voor het opstellen van het informatiebeveiligingsbeleid.
- Teams zijn verantwoordelijk voor het toepassen en de uitvoering van het informatie- en informatiebeveiligingsbeleid
- Medewerkers zijn verantwoordelijk voor hun eigen gedrag en voor de naleving van procedures

Taken

- **Het College:** stelt het informatiebeleid en het informatiebeveiligingsbeleid vast en zorgt voor de resources om hier uitvoering aan te geven
- **De informatiemanager (CIO):** geeft namens de directie 'handen en voeten' aan het informatiebeleid, treedt adviserend en coördinerend op het gebied van informatiemanagement, houdt toezicht op de algehele werking van het informatiebeleid en faciliteert de implementatie van dit beleid
- **De CISO:** geeft namens de directie 'handen en voeten' aan informatiebeveiliging, treedt adviserend en coördinerend op het gebied van informatiebeveiliging, houdt toezicht op de algehele werking van het informatiebeveiligingsbeleid en faciliteert de implementatie van dit beleid
- **Teamleiders:** zien er op toe dat informatiebeleid en informatiebeveiligingsbeleid tot uitvoering wordt gebracht
- **Medewerkers:** verantwoordelijk gedragen, elkaar aanspreken op gedrag en werken aan bewustwording

Asten "In control"

Het beheren, het in kaart brengen en begrijpen van de risico's van de assets (middelen) is voor een organisatie een cruciaal onderdeel van de informatiebeveiligings-cyclus. De informatiebeveiligings-cyclus kent een continue proces en bestaat uit de volgende onderdelen:

- Identificatie van assets
- Beschermen van assets
- Detecteren van incidenten
- Acteer en voer uit volgens plan
- Herstellen en opnieuw testen

Het naleven van deze aspecten binnen de informatiebeveiligings-cyclus moet Asten een betere controle kunnen geven over de beveiliging van informatie van de diverse assets.
We evalueren dit per jaar en rapporteren hierover.
ENSIA toetst hierop.



Opbouw informatiebeveiligingsbeleid

In 2024 wordt er een nieuw informatieveiligheidsbeleid gemaakt en vastgesteld.

Onderstaande onderdelen komen hier in terug:

- De visie en algemene uitgangspunten
- Organisatie van de informatiebeveiliging
- Toegangsbeveiliging beleid
- Beheer van beveiligingsincidenten
- Bewustzijn programma voor medewerkers

De Baseline Informatiebeveiliging Overheid (BIO) wordt als kader gebruikt.

Operationeel/Verrichten per jaar

Hoofd activiteiten 2024

Beleid

- Informatiebeleid uitvoeren en in organisatie laten landen
 - Informatiebeveiligingsbeleid vaststellen
- Q1 – Q2 2024

Organisatie

- Inrichting van de CISO en CIO rol
 - Doorontwikkeling van informatiemanager rollen
- Q1 – Q4 2024
- Opleiden functioneel beheer
- Q1 - Q2 2024



Software

- Implementatie zaakstelsysteem
- Q1 – Q2 2024
- Implementatie financiële applicatie (verlengd tot 2025)
- 2024 – 2025

Hardware

- Implementatie audiovisuele middelen gemeentehuis Asten 2024

Vaardigheid

- Digivaardigheid trainingen (wisselende onderwerpen)
 - Bewustwording m.b.t. informatieveiligheid en privacy
- Q1 – Q4 2024

Structureel

Prioriteit het komende jaar voor team I:

- **Digivaardigheid bij medewerkers verhogen.** Het trainen van medewerkers in het gebruik van de nieuwe werkomgeving. Wanneer dit goed gebeurt dan heeft dit ook een positieve uitwerking op cybersecurity. We ontwikkelen hiermee naar "bewust bekwaame" medewerkers;
- **Evaluatie van de ICT migratie van GSA naar ICT NML.** Nu de overgang naar ICT NML is afgerond is het belangrijk dat deze geëvalueerd wordt: hoe staat het met de (klant)tevredenheid en wat staat er nog op de planning?
- **Implementatie zaakstelsysteem.** Met de inrichting van het nieuwe zaakstelsysteem gaan we terug naar de basis. Binnen de organisatie wordt het belang van zaakgerichtwerken opnieuw onder de aandacht gebracht. Ook bekijken we opnieuw het aantal zaaktypen en de te archiveren documenten.
- **Bewustwording rond informatieveiligheid en privacy.** Door het tempo waarmee digitalisering zich ontwikkelt neemt ook het risico toe op cybercrime. Technisch kunnen we veel beveiligen, maar dit gaat altijd samen met menselijk gedrag. Dit betekent dat we gebruikers moeten blijven informeren en trainen in bewustwording van informatieverwerking.

6 expertise gebieden van informatiebeleid

Het informatiebeleidsveld wordt ingevuld vanuit verschillende rollen en functies. Doordat digitalisering toeneemt is ook de verwevenheid tussen informatie, veiligheid en privacy toegenomen. Betekent dat een integrale aanpak nodig is van onderstaande expertise gebieden. Dit moet de komende jaren verder ontwikkeld worden.

Informatiemanagement

Vertalen van de informatiebehoeften (die uit de verschillende werk- en bedrijfsprocessen van de organisatie ontstaan) naar de informatievoorziening die deze processen optimaal ondersteunt.

Procesmanagement

Vastleggen en optimaliseren van (primaire) organisatieprocessen. Het eigenaarschap van de processen is en blijft van het werkveld zelf.

Gegevensbescherming

Afhandelen van risico's rond gegevensbescherming en AVG-gerelateerde vraagstukken gedicteerd vanuit een gemeente breed programma rondom gegevensbescherming.

Recordmanagement

Borgen en het op orde houden van de (in de processen gebruikte) informatie in het kader van vernietiging, toegankelijkheid, terugvindbaarheid, archivering en de Wet Open Overheid.

Domeinarchitectuur

Optekenen van de informatie-architectuur en bewaken van kaders waaraan de infrastructuur en (technische) oplossingen moeten voldoen. Dit ook bekeken vanuit de verschillende domeinen.

Informatieveiligheid

We gebruiken de Baseline Informatiebeveiliging Overheid (BIO). Dit is het normenkader voor informatiebeveiliging waaraan de gemeente zich conformeert en biedt volop ruimte voor risicoafweging en prioritering voor verbetering. Een praktische vertaling naar een actieplan moet ervoor zorgen dat informatieveiligheid een continu proces blijft.