GEMEENTE Asten
GEMEENTEBLAD
Officiële uitgave van de gemeente Asten

Nr. 518871
13 december
2024

Informatiebeveiligingsbeleid 2024 - 2026 gemeente Asten

Inleiding

Met dit Informatiebeveiligingsbeleid 2024 - 2026 gemeente Asten zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. Dit beleid ziet op de jaren 2024 tot en met 2026 en vervangt het op 15 december 2021 vastgestelde informatiebeveiligingsbeleid (documentnummer 2021073666). De basis voor dit beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Dit informatiebeveiligingsbeleid is gebaseerd op de tien principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage 1.

Leeswijzer

In hoofdstuk 2 wordt de kern van het informatiebeveiligingsbeleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit informatiebeveiligingsbeleid. In het jaarlijks uit te brengen gemeentelijk informatiebeveiligingsjaarplan (vast te stellen door het MT) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teamleiders, de PO, de CIO, de CISO, het dreigingsbeeld van de IBD, het jaarverslag informatiebeveiliging en de uitkomsten van ENSIA. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernaspecten hierbij zijn:

Vertrouwelijkheid: Zorgt ervoor dat informatie alleen toegankelijk is voor geautoriseerde personen of systemen.
Integriteit: Garandeert de nauwkeurigheid en volledigheid van informatie door te voorkomen dat deze ongeautoriseerd wordt gewijzigd.
Beschikbaarheid: Zorgt ervoor dat informatie beschikbaar is voor geautoriseerde gebruikers wanneer ze het nodig hebben.
Bewustwording en training: Het betrekken van medewerkers bij beveiligingspraktijken en hen voorzien van de nodige kennis en vaardigheden om veilig met informatie om te gaan.

Het informatiebeveiligingsbeleid geldt voor de gehele organisatie, wat zowel de gemeentelijke organisatie als de gemeenteraad omvat. Informatiebeveiliging is van cruciaal belang voor het beschermen van gevoelige informatie, ongeacht waar deze zich binnen de organisatie bevindt.

Ambitie en visie op gebied van informatieveiligheid

Belangrijk is om vast te stellen waar de gemeente Asten nu staat. Van daaruit zal verder worden gekeken waar Asten naartoe wil. Voorop staat dat Asten in ieder geval ernaar streeft om de basis op orde te hebben en te voldoen aan de BIO.

Doel

Het informatiebeveiligingsbeleid heeft als doel de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. Enkele specifieke doelen en redenen waarom zijn:

- **Bescherming van gevoelige informatie**:
  Gemeenten verwerken en beheren gevoelige informatie, waaronder persoonsgegevens van burgers, financiële gegevens en andere vertrouwelijke informatie. Het primaire doel is ervoor te zorgen dat deze informatie niet ongeoorloofd wordt onthuld of gewijzigd.
- **Voorkomen van datalekken**:
  Door informatiebeveiligingsmaatregelen te implementeren, tracht een gemeente het risico op datalekken te minimaliseren. Dit omvat onbedoelde of kwaadwillige openbaarmaking van gegevens.

- **Beschikbaarheid van diensten garanderen**:
  Het beleid is erop gericht ervoor te zorgen dat essentiële diensten en systemen beschikbaar blijven. Dit voorkomt verstoringen door bijvoorbeeld cyberaanvallen of technische storingen.
- **Bewustwording en training**:
  Het beleid omvat vaak maatregelen om bewustzijn over informatiebeveiliging te vergroten en training te bieden aan medewerkers. Menselijke fouten vormen vaak een zwakke schakel in informatiebeveiliging, en training kan deze risico's verminderen.
- **Vertrouwen van burgers en partners behouden**:
  Het succes van een gemeente hangt in grote mate af van het vertrouwen van burgers en samenwerkingspartners. Een sterk informatiebeveiligingsbeleid draagt bij aan het behouden van dit vertrouwen door een zorgvuldige omgang met informatie.

Over het algemeen draagt informatiebeveiligingsbeleid bij aan de bescherming van kritieke informatie, zorgt het voor naleving van wet- en regelgeving en versterkt het vermogen van de gemeente om met moderne beveiligingsuitdagingen om te gaan.

Het informatiebeveiligingsbeleid wordt verder uitgewerkt in concrete maatregelen die we jaarlijks bij stellen in het Informatiebeveiligingsjaarplan 2024. Daarnaast zijn er 10 basisprincipes opgesteld voor veilig werken zie bijlage 2.

Ontwikkelingen

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

De BIO
De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teamleiders nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het MT in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.
Gedurende de implementatie van dit informatiebeveiligingsbeleid 2024 – 2026 gemeente Asten zal de BIO 2.0. op basis van NEN-EN-ISO/IEC 27002:2022 van kracht worden. Implementatie start in 2024.

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

Informatie uit incidenten en inbreuken op de beveiliging
De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem, met het zaaksysteem als belangrijkste bron, geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

NIS2, Network and Information Security
De nieuwe Network and Information Systems Directive (NIS2-richtlijn) heeft belangrijke implicaties voor gemeenten als het gaat om toezicht op informatiebeveiliging. De richtlijn is sinds begin 2023 van kracht. EU-lidstaten zijn verplicht deze uiterlijk 17 oktober 2024 in nationale wetgeving om te zetten. Ook gemeenten vallen onder de reikwijdte van de NIS2.
Gezien het feit dat gemeenten nu al een zorgplicht, een meldplicht (de Informatiebeveiligingsdienst, IBD) en toezicht hebben zal de impact van NIS2 voor gemeenten afhankelijk zijn van de mate waarin nu al gedocumenteerd voldaan wordt aan de BIO. Daarom is het cruciaal dat de gemeente Asten door blijft gaan met de cyclus van plannen, uitvoeren, controleren en bijstellen rondom de complete BIO.

Plaats van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.
Dit informatiebeveiligingsbeleid wordt vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in een jaarlijks op te stellen document, het “Informatiebeveiligingsjaarplan [jaar]”.

Daarbij is het van belang de rollen en taken van deze personen te onderscheiden van verantwoordelijkheden. Procesverantwoordelijken dragen de verantwoordelijkheid voor het beheer, de uitvoering en de verbetering van een specifiek bedrijfsproces en moeten zich laten adviseren door de personen uit de driehoek Informatieveiligheid / Informatiemanagement / Privacy (zie volgende pagina). Teamleiders moeten hierop sturen door de proceseigenaren bij hun rol te ondersteunen en indien nodig daarop aan te spreken.
Teamleiders monitoren op voortgang en prestaties. Daarnaast geven ze richting door de proceseigenaren te ondersteunen in hun rol.

Informatieveiligheid, privacy en informatiemanagement wordt met de volgende functies ingevuld binnen Asten.

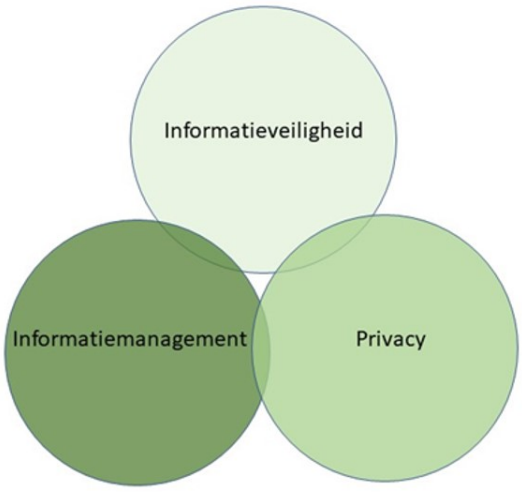
Functionaris voor Gegevensbescherming (FG): is verantwoordelijk voor het waarborgen van de naleving van privacywetgeving binnen een organisatie. Adviseert over en bewaakt de implementatie van beleid en procedures met betrekking tot gegevensbescherming.

Privacy Officer (PO): is verantwoordelijk voor het ontwikkelen, implementeren en handhaven van het privacy-beleid van de organisatie. Coördinatie van privacy-activiteiten, waaronder het beheer van gegevensverwerkingsactiviteiten en het waarborgen van de juiste naleving van privacywetten, behoort tot de taken.

Chief Information Security Officer (CISO): de CISO is belast met het ontwikkelen, implementeren en handhaven van het informatiebeveiligingsbeleid van een organisatie. Ze leiden inspanningen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. De CISO coördineert beveiligingsmaatregelen, leidt incidentresponsactiviteiten en adviseert het leiderschap over strategische beveiligingskwesties.

Chief Information Officer / informatiemanager (CIO): de CIO is verantwoordelijk voor de algehele informatiestrategie van een organisatie. Neemt strategische beslissingen met betrekking tot technologie-investeringen. De CIO zorgt ervoor dat technologische oplossingen naadloos integreren met de bredere organisatiestrategie. Is verantwoordelijk voor het beheer van IT-projecten en programma's om de doelen van de organisatie te ondersteunen.

De samenhang tussen informatiemanagement, informatiebeveiliging en privacy is cruciaal in het hedendaagse digitale tijdperk waarin gegevens een centrale rol spelen in een organisatie en samenleving. De samenhang is essentieel om ervoor te zorgen dat organisatie voldoen aan wettelijke vereisten, de vertrouwelijkheid van informatie behouden en zichzelf beschermen tegen datarisico's en bedreigingen. Zie onderstaand plaatje.



Scope informatiebeveiliging

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

Dit Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP, BAG en SUWI (respectievelijk: Basisregistratie Personen, Basisregistratie Adressen en Gebouwen en Wet structuur uitvoeringsorganisatie werk en inkomen). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.
In de onderliggende documenten wordt de link naar dit informatiebeveiligingsbeleid gelegd.
Dit geldt voor alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.

Uitgangspunten

Het college van burgemeester en wethouders, het MT en de teamleiders spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Het MT maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het MT dit beleid voor informatiebeveiliging om, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

MT en teamleiders geven een duidelijke richting aan informatiebeveiliging en dragen dit uit. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, informatiesystemen, procesautomatisering en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

Strategische doelen
De strategische doelen van het informatiebeveiligingsbeleid zijn:

- **Bescherming van gevoelige gegevens:** Het waarborgen van de vertrouwelijkheid van persoonsgegevens, financiële informatie, en andere gevoelige gegevens van burgers en de gemeente zelf tegen ongeautoriseerde toegang, gebruik of openbaarmaking.
- **Bescherming tegen cyberdreigingen**: Het beschermen van de gemeentelijke systemen, netwerken en infrastructuur tegen cyberaanvallen, malware, phishing en andere vormen van kwaadaardige activiteiten die de operationele continuïteit kunnen bedreigen.
- **Bescherming van kritieke infrastructuur**: Het waarborgen van de beschikbaarheid en integriteit van kritieke gemeentelijke systemen en diensten, zoals water- en energievoorziening, verkeersregelingssystemen en noodhulpdiensten, tegen verstoringen en aanvallen.
- **Compliance met wet- en regelgeving**: Het voldoen aan relevante wet- en regelgeving op het gebied van gegevensbescherming, privacy, en informatiebeveiliging, zoals de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- **Vertrouwen van belanghebbenden**: Het opbouwen en behouden van vertrouwen bij burgers, bedrijven, en andere belanghebbenden door te laten zien dat de gemeente zorgvuldig omgaat met hun informatie en dat hun privacy en veiligheid worden beschermd.

Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van burgemeester en wethouders is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Asten hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsjaarplan en het informatiebeveiligingsjaarverslag het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsjaarplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Elke medewerker, ongeacht hun status (vast of tijdelijk), interne of externe positie, heeft de verantwoordelijkheid om gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, wijziging, openbaarmaking, vernietiging, verlies of overdracht. In geval van vermoedelijke schendingen van deze beveiligingsmaatregelen, wordt van hen verwacht dat zij dit melden.

Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van burgemeester en wethouders stelt als eindverantwoordelijke het informatiebeveiligingsbeleid vast.
- Het MT stelt jaarlijks het “Informatiebeveiligingsjaarplan [jaar]” en het jaarverslag informatiebeveiliging vast.
- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Het MT is belast met het aanvragen van informatie bij de teamleiders en zorgt ervoor dat de teamleiders passende maatregelen hebben genomen ter bescherming van de informatie, informatiesystemen en geautomatiseerde processen die onder hun verantwoordelijkheid vallen.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het MT.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- Teamleiders zien erop toe dat proceseigenaren hun verantwoordelijkheid nemen ten aanzien van informatiebeveiliging bij de processen waar zij verantwoordelijk voor zijn.
- Het MT is verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, SUWI, BAG, WOZ, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden doorlopend getraind en krijgen instructie op gebied van informatieveiligheid en privacy. Resultaten worden aan het MT gerapporteerd.
- Informatiebeveiliging maakt deel uit van het ontwikkelgesprek en wordt besproken tussen de teamleider en de medewerker.

Randvoorwaarden
Belangrijke randvoorwaarden zijn:
- Informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsjaarplan opgesteld onder leiding van de CISO, gebaseerd op:
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Het jaarverslag informatiebeveiliging;
    - Het dreigingsbeeld gemeenten van de IBD;
    - De door de teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van het te implementeren dashboard.

Taken en verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO) ondersteunt, adviseert, coördineert en bewaakt

of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering. In bijlage 3 een uitwerking van de interne onderlinge samenwerking.

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

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

Uitvoering: teamleiders
De teamleiders dragen de verantwoordelijkheid voor informatiebeveiliging binnen hun teams. Om deze verantwoordelijkheid effectief te kunnen vervullen, is het essentieel dat zij worden ondersteund vanuit de CISO. Hoewel zij de uitvoerende taken kunnen delegeren, blijven zij altijd verantwoordelijk voor alle processen, data en applicaties binnen hun team. Daarom wordt ervoor gezorgd dat elk aspect altijd minstens één eigenaar heeft, en deze verantwoordelijkheden worden gedocumenteerd. Momenteel wordt dit bijgehouden in iNavigator, maar dit kan in de toekomst veranderen.
De teamleiders rapporteren regelmatig aan het MT over de tactische en operationele activiteiten die zij hebben uitgevoerd met betrekking tot informatiebeveiliging. Om ervoor te zorgen dat de aanpak op elkaar is afgestemd, wordt het onderwerp informatiebeveiliging minstens vier keer per jaar besproken tijdens MT/TL, waarbij ook afstemming plaatsvindt met de andere afdelingen.

Taken van de teamleiders in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wetgeving die op de processen die binnen hun team plaatsvinden van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Controle en verantwoording
Dit Informatiebeveiligingsbeleid is een verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Asten. Het MT en teamleiders van de gemeente Asten zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
Het MT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het MT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit beleid. Zie bijlage 4 voor verantwoordingsmatrix.

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

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

Middels deze verantwoording worden het college van burgemeester en wethouders en de gemeenteraad van de gemeente Asten geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat

de gemeente Asten informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Bijlage 1 - De 10 bestuurlijke principes voor informatiebeveiliging

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1 Bestuurders bevorderen een veilige cultuur
Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.
Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.
Toelichting
Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2 Informatiebeveiliging is van iedereen
Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.
Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.
Toelichting
Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Privacy Officer (PO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3 Informatiebeveiliging is risicomanagement
Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.
Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.
Toelichting
Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming
Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.
Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.
Toelichting
U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.
Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.
Toelichting
Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6 Informatiebeveiliging is een proces
Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.
Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.
Toelichting
Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7 Informatiebeveiliging kost geld
Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.
Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.
Toelichting
Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve-en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8 Onzekerheid dient te worden ingecalculeerd
De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.
Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.
Toelichting
Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9 Verbetering komt voort uit leren en ervaring
Risicobeheer wordt voortdurend verbeterd door leren en ervaring.
Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.
Toelichting
Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10 Het bestuur controleert en evalueert
Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.
Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te

weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie.

Bijlage 2 - 10 basisprincipes voor veilig werken

1 **Meld incidenten in EVA als:**
- onbevoegden (mogelijk) vertrouwelijke informatie in handen hebben gekregen (datalek);
- je technische incidenten zoals inbraak, verlies of diefstal constateert;
- je twijfelt of een gebeurtenis een incident is.

2 **Begeleid bezoekers en spreek onbekenden aan**

3 **Let goed op je toegangspas, dit is een sleutel**
- Meld direct bij personeelszaken wanneer je de pas kwijt bent of je een pas gevonden hebt.
- Zorg ervoor dat je pas niet herleidbaar is naar de gemeente.

4 **Wees oplettend wanneer je werkt met informatie**
- Vertrouwelijke informatie? Zorg ervoor dat niemand mee kan kijken of luisteren.
- Wees alert op telefoontjes, verstrek geen (persoons)gegevens wanneer je niet 100% zeker weet dat je de juiste persoon aan de telefoon hebt.
- Deponeer fysieke documenten met vertrouwelijke gegevens niet in de prullenbak. Maar behandel ze volgens de afgesproken werkwijze
- Deel geen vertrouwelijke informatie via de reguliere mail, social media, Dropbox, WeTransfer, Trello en soortgelijke programmatuur, maar gebruik Zorgmail (of een vervanger daarvan zoals Bastion365).

5 **Zorg voor een cleandesk en –screen**
- Berg vertrouwelijke documenten op wanneer je de werkplek verlaat.
- Vergrendel altijd je beeldscherm wanneer je niet achter je beeldscherm zit (ook thuis).
- Berg waardevolle privé eigendommen zoals tassen, sleutels en portemonnees op.

6 **Houd je wachtwoorden altijd geheim, deel deze ook niet met collega's**
- Wijzig je wachtwoord wanneer deze (vermoedelijk) is gelekt.
- Gebruik hetzelfde wachtwoord niet voor verschillende toepassingen.
- Schrijf je wachtwoorden niet (digitaal) op. Maar stop die in de door, de werkgever beschikbaar gestelde, wachtwoordkluis
- Gebruik, voor zover de programmatuur dat toelaat overal 2-factor authenticatie.
- Toegang tot een systeem of mailbox van je collega nodig? EVA helpt je, na overleg met de CISO en de PO, hierbij.

7 **Beveilig (privé) apparatuur**
- Denk hierbij aan het instellen van een wachtwoord, pincode, antivirussoftware et cetera.
- Meld verlies van je werklaptop, -tablet of -mobiel direct in EVA.
- (Laat) zakelijke gegevens wissen voor inleveren, afgifte of reparatie van apparatuur.

8 **Werk veilig met digitale gegevensdragers en mobiele apparaten**
- Laat telefoons, tablets en laptops niet onbeheerd achter.
- Gebruik geen onbekende (open) Wifi-netwerken.
- Gebruik geen USB-sticks, zeker geen onbeveiligde of gevonden USB-sticks. Voor dataoverdracht naar bijvoorbeeld het streekarchief eerst overleg met de CISO.
- Plaats geen bestanden, en zeker niet met vertrouwelijke informatie, op mobiele apparaten.

9 **Wees alert op websites en e-mails**
- Open geen verdachte bestanden.
- Klik niet op verdachte links, pop ups, afbeeldingen. En scan geen onbekende QR-codes
- Bel direct de CISO of het servicepunt van ICT NML wanneer je vermoedt dat je apparaat of digitale werkomgeving mogelijk is geïnfecteerd. Of er zich een andere onregelmatigheid heeft voorgedaan.

10 **Werk je met persoonsgegevens? Ga hier bewust mee om**
- Vraag niet meer persoonsgegevens op dan nodig.
- Gebruik persoonsgegevens niet voor een ander doel dan waarvoor ze zijn verzameld.
- Vraag je af of je het doel kunt bereiken zonder persoonsgegevens.
- Deel persoonsgegevens niet zomaar met derden.
- Bewaar persoonsgegevens niet langer dan de wettelijke bewaartermijn

Bijlage 3 - Uitgangspunten samenwerking

1. In geval van een crisissituatie is de burgemeester altijd portefeuillehouder. Gemeentesecretaris en burgemeester zijn daarom altijd in de lead.
2. Opdrachten aan de ambtelijke organisatie worden altijd door de gemeentesecretaris verstrekt. Een uitzondering daarin is een crisissituatie. In dat geval mag de burgemeester rechtstreeks een opdracht geven. Maar in Asten laten we dat, indien de situatie het toelaat, ook dat via de gemeentesecretaris lopen.
3. We mogen meningsverschillen hebben en verschil van inzicht. Maar we behandelen elkaar altijd met respect. Naar buiten toe spreken we met één mond.
4. Afgrenzing tussen crisis enerzijds en regulier beleid/uitvoering anderzijds gebeurt in overleg tussen de portefeuillehouders.
5. Principe van integrale advisering: alle disciplines zijn betrokken, geven standpunten en vervolgens wordt er één advies gemaakt, met de mogelijkheid om de verschillende standpunten weer te geven (ivm mogelijke alternatieven en risico's). Er gaat dus maar één standpunt naar buiten de gemeente Asten. Dit is belangrijk om ons eigen standpunt en onze positie niet te ondermijnen of een negatief beeld te voorkomen over de kwaliteit van onze besluitvorming.
6. We informeren elkaar volledig en tijdig. Kennis is alléén macht als dit gedeelde kennis is. Dit is ook nodig voor het principe van integrale advisering.

Bijlage 4 - Verantwoordingsmatrix

	MT	College	Gemeenteraad
Meerjarenbeleid	Betrekken	Vast laten stellen	Informeren
Jaarplan	Vast laten stellen	Informeren	--
ENSIA	Betrekken	Vast laten stellen	Informeren (onder geheimhouding)
Verbeterplan ENSIA	Vast laten stellen	--	--
Jaarverslag informatiebeveiliging	Vast laten stellen	Informeren	--