Informatiebeveiligingsbeleid 2023-2026

Op weg naar een weerbaar huis van de stad

September 2022

CLASSIFICATIE: OPENBAAR

Stad met een hart

Amersfoort

Inhoudsopgave

1 Inleiding en ambities

1.1 Achtergrond

Voor het uitvoeren van de gemeentelijke processen is een betrouwbare informatievoorziening essentieel. Betrouwbaar houdt niet alleen in dat de informatie op het juiste moment beschikbaar is, maar ook dat de informatie juist is. Aangezien veel gemeenteprocessen informatie van burgers verwerken, is het zeker zo belangrijk dat alleen diegene bij de informatie kan die het nodig heeft om de gemeentelijke taken uit te voeren.

Burgers, bedrijven en verbonden partijen mogen van de gemeente Amersfoort verwachten dat zij zorgvuldig omgaat met informatie en (persoonlijke) gegevens, zowel intern als in de samenwerking met derde partijen.

1.2 De BIO

De Baseline Informatiebeveiliging Overheid (BIO) is sinds 1 januari 2020 het vigerende normenkader voor de hele overheid. De werkwijze van de BIO staat voor een risico gebaseerde aanpak. Dit betekent concreet dat het management op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

1.3 Doelstellingen

De gemeente Amersfoort wil een solide en betrouwbare partner zijn voor haar inwoners, bedrijven, keten- en regiepartners en derden vanuit haar verantwoordelijkheid voor gegevens en informatie. Dit resulteert in de volgende doelstellingen:

- Medewerkers, inwoners, bedrijven en instellingen weten dat hun gegevens veilig zijn;
- De dienstverlening is betrouwbaar en verloopt onverstoord;
- Medewerkers zijn privacy- en beveiligingsbewust en beschikken over de juiste kennis en middelen om hun verantwoordelijkheid voor informatiebeveiliging te nemen;
- De gemeente is aantoonbaar *in control* op informatiebeveiliging. Dit betekent dat de gemeente weet welke passende technische en organisatorische beveiligingsmaatregelen er al zijn en welke nog moeten worden ingericht of waar bewust wordt afgeweken.

1.4 Bedreigingen en ontwikkelingen

Amersfoort is aangesloten bij de gemeentelijke informatiebeveiligingsdienst (IBD). Jaarlijks publiceert de IBD in samenwerking met het National Cyber Security Center (NCSC) een 'dreigingsbeeld' op het terrein van cyber security. In het dreigingsbeeld 2021/2022[1] zijn de vier belangrijkste dreigingen voor gemeenten geïdentificeerd:

1. extern en gericht, bijvoorbeeld doelgerichte pogingen om geld of informatie buit te maken;
2. extern en ongericht, bijvoorbeeld grootschalige phishing- en ransomwarecampagnes;
3. intern en onbedoeld, bijvoorbeeld fouten van medewerkers met incidenten als gevolg;
4. intern en gericht, bijvoorbeeld fraude en ondermijnende activiteiten van eigen medewerkers.

Amersfoort onderkent deze dreigingen en heeft in de afgelopen beleidsperiode gewerkt aan een basis die de gemeente in staat stelt om op alle risicogebieden door te groeien. Informatiebeveiliging is een regelmatig terugkerend onderwerp op de managementagenda's. Dit is een randvoorwaarde voor risicomanagement en controle op informatiebeveiliging. Daarnaast zijn het werken 'in regie' en werken via 'Cloud' belangrijke ontwikkelingen waarbij het belang van controle, audit en rapportage toeneemt. Aan de hand van drie speerpunten geeft de gemeente de komende jaren richting aan een effectief en doeltreffend informatiebeveiligingsbeleid.

1.5 Speerpunten voor de komende beleidsperiode

In deze beleidsperiode zet de gemeente in op drie speerpunten voor informatiebeveiliging. De speerpunten vormen de kaders en deze worden verder uitgewerkt op basis van het risicomanagementproces. Naast de drie speerpunten hanteert gemeente Amersfoort een aantal leidende principes die richting geven aan de invulling van informatiebeveiliging. Deze leidende principes worden in hoofdstuk drie toegelicht.

Speerpunt 1: Het belang voor informatiebeveiliging is duidelijk voor iedereen
Het beschermen van informatie is een verantwoordelijkheid van iedereen. Je kunt kan pas verantwoordelijkheid nemen als je weet wat er verwacht wordt en welke mogelijke gevaren er zijn. Het is daarom essentieel dat medewerkers getraind zijn en blijven op het gebied van informatiebeveiliging. De structurele bewustwording resulteert in een verhoogde weerbaarheid tegen de steeds veranderende Social Engineering[2] aanvallen. Het beveiligingsbewustzijn wordt een onderdeel van de manier van werken en daarmee creëren we een sterke menselijke schakel in informatiebeveiliging.

Speerpunt 2: Technische maatregelen groeien mee met het cyber dreigingsbeeld
Naast een goed beveiligingsbewustzijn, beschermt een scala aan technische beveiligingsmaatregelen de gemeentelijke informatie. Dit begint met een goede inrichting van de basismaatregelen uit de verplichte normenkaders zoals BIO[3], DigiD en Suwinet.

De digitale dreigingen ontwikkelen zich continue, waardoor aanvallers bestaande barrières weten te doorbreken of te omzeilen. Een beveiligingsmaatregel die een aantal jaar geleden nog voldoende bescherming bood, schiet nu mogelijk te kort. Om mee te blijven groeien en in de pas te blijven met het cyber dreigingsbeeld, is het zaak om de technische beveiligingsmaatregelen voortdurend te blijven controleren op effectiviteit. Deze controle vindt onder andere plaats door de actuele ontwikkelingen in het cyber security domein op de voet te volgen, het regelmatig (laten) uitvoeren van penetratietesten en in- en externe audits.

[1] https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2021-2022/
[2] Social Engineering is de aanvalsmethode die gericht is op het uitbuiten van zwakheden in de menselijke factor.
[3] Baseline Informatiebeveiliging Overheid, een overzicht van de aandachtsgebieden is opgenomen in bijlage II.

Bij het adopteren van nieuwe technologieën wordt er al in een vroeg stadium gekeken naar informatiebeveiligings- en privacy risico's. Hierbij wordt niet alleen rekening gehouden met de security en privacy principes *Privacy and Security by Design and by Default,* maar ook met de Notitie IV *'by design*'. Geïdentificeerde risico's worden inzichtelijk gemaakt zodat risico-afweging en inpassen van maatregelen kan plaatsvinden.

Speerpunt 3: Planning en Control cyclus (P&C) **voor informatiebeveiliging is ingericht voor alle afdelingen**
De komende periode wordt de P&C cyclus verder doorontwikkeld, zodat de P&C cyclus voor informatiebeveiliging tot op afdelingsniveau is ingericht.

De afdelingsmanagers zijn verantwoordelijk voor informatiebeveiliging binnen hun afdeling. Dit stelt hen in staat om zelf maatregelen te treffen en risico's binnen de afdeling af te wegen. Over de informatiebeveiliging legt de afdelingsmanager verantwoording af aan de CISO en de directie. De directie stelt de gemeente brede verantwoording vast. Op basis van de gemeente brede verantwoording worden het college en de gemeenteraad geïnformeerd.

1.6 Algemene beleidsuitgangspunten

Voor de uitvoering van het Informatiebeveiligingsbeleid worden de volgende uitgangspunten gehanteerd:

- Het Informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante nationale en Europese wet- en regelgeving (zie bijlage III);
- Er wordt gewerkt volgens de Baseline Informatiebeveiliging Overheid (BIO), deze wordt jaarlijks getoetst via de ENSIA;[4]
- Het Informatiebeveiligingsbeleid is in lijn met het privacy beleid van de gemeente Amersfoort.

1.7 Ambitieniveau

Het ambitieniveau van de gemeente Amersfoort is om te bouwen op het fundament van informatiebeveiliging. Dit leidt tot een beveiligingsbewuste organisatie die weet welke risico's er zijn, wat er wordt gedaan en wat nog moet worden gedaan om deze risico's te beheersen in lijn met de BIO.

1.8 Reikwijdte

Het Informatiebeveiligingsbeleid geldt voor het hele proces van informatievoorziening en voor alle informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT-organisatie, maar heeft ook betrekking op het bestuur, alle medewerkers en de keten- en regiepartners. Het beleid raakt daarnaast ook burgers en bedrijven wanneer zij transacties doen met de gemeente.

[4] ENSIA staat voor Eenduidige Normatiek Single Information Audit. (https://ensia.nl)

2 Achtergronden bij Informatiebeveiliging in Amersfoort

2.1 Betrouwbaarheid van informatie

Informatieveiligheid omvat de processen die leiden tot een informatieveilige gemeente. Informatiebeveiliging is de verzamelnaam voor de processen die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Dit betreft onder andere maatregelen op het gebied van uitwijk voorzieningen, regels en afspraken rond toegang tot systemen, fysieke toegangsbeveiliging, beveiligingsorganisatie, et cetera. Bij informatiebeveiliging staan de volgende begrippen centraal:

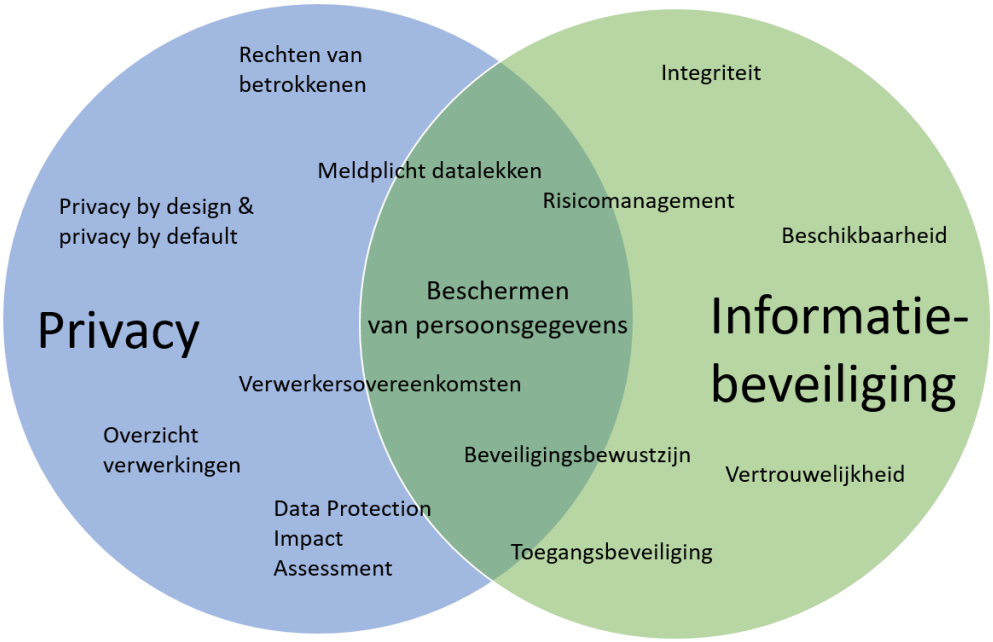
- **Beschikbaarheid**
  Het zorgdragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;

- **Integriteit**
  Het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;

- **Vertrouwelijkheid**
  Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

2.2 Informatiebeveiliging in relatie tot privacy

De taakvelden privacy en informatiebeveiliging werken nauw samen. Burgers hebben recht op eerbiediging en bescherming van de persoonlijke levenssfeer en een zorgvuldige omgang met hun persoonsgegevens. Dit vraagt om een adequate beveiliging van deze persoonsgegevens en het respecteren van de privacy wetgeving. Het beschermen van persoonsgegevens vormt een gemeenschappelijke domein waar privacy en informatiebeveiliging samenkomen.



Op Europees niveau zijn de privacy regels in de General Data Protection Act vastgesteld, op nationaal niveau is dat de Algemene Verordening Gegevensbescherming (AVG). De gemeente Amersfoort voldoet aan de

eisen van de AVG en heeft passende technische en organisatorische maatregelen getroffen om persoonsgegevens adequaat te beschermen. Dit Informatiebeveiligingsbeleid beschrijft hoe de informatie van de gemeente wordt beschermd, inclusief persoonsgegevens. Het borgen van de privacy-aspecten van persoonsgegevens is vastgelegd in het privacy beleid.

3 Leidende principes

De gemeente Amersfoort hanteert een aantal leidende principes. Deze zijn mede gebaseerd op de 10 principes voor informatiebeveiliging (zie bijlage I) op basis waarvan richting wordt gegeven aan informatiebeveiliging in onderliggende beleidsdocumenten.

3.1 Risicogericht werken

Risicogericht werken zorgt ervoor dat risico's inzichtelijk zijn en weloverwogen keuzes gemaakt worden op basis van een acceptabel risico. De afdelingsmanagers voeren risico sessies uit om de risico's binnen de afdeling te identificeren. De risico's en de behandeling daarvan zijn een vast onderdeel van de managementverantwoording van de manager aan de CISO. Daar waar risico's afdeling overstijgend zijn zal de directie worden geïnformeerd door de CISO.

Het melden van beveiligingsincidenten is een belangrijke basis voor risicogericht werken. Er is een verplichte meldingssystematiek ingericht om alle informatiebeveiligingsincidenten en datalekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon. Alle beveiligingsincidenten worden geregistreerd. Bij elk (potentieel) beveiligingsincident wordt direct beoordeeld of het een datalek betreft. Specifiek voor datalekken is een protocol opgesteld dat waarborgt dat een datalek op de juiste wijze wordt geregistreerd en binnen de gestelde termijn wordt gemeld aan de autoriteit persoonsgegevens (AP).

3.2 Classificeren van informatie

Informatie wordt geclassificeerd om te bepalen welke beveiligingsmaatregelen nodig zijn. Hierbij is de aard van de informatie in de processen leidend. Er wordt geclassificeerd op de drie betrouwbaarheidsaspecten van informatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

Op basis van een classificatie wordt bepaald hoe deze informatie behandeld dient te worden. De gemeente Amersfoort onderscheidt vier classificatieniveaus[5], te weten Geheim, Vertrouwelijk, Bedrijfsvertrouwelijk en Openbaar. De classificatieniveaus zijn vastgelegd in een classificatieschema, inclusief de voorwaarden om de informatie te verwerken.

3.3 Externe samenwerkingen

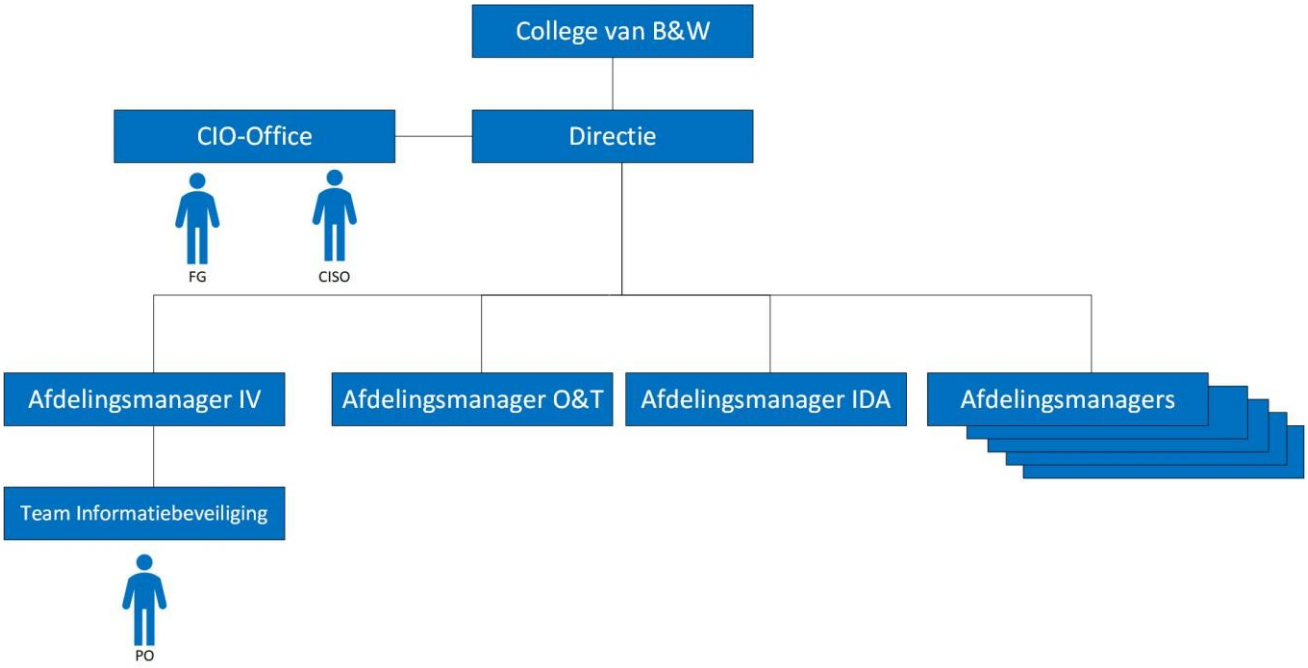
Externe actoren en de bijbehorende bedreigingen zijn zeer divers en hebben voldoende tijd, kennis en middelen om hun doelen te realiseren. Organisaties die zich willen beschermen, hebben slechts een beperkte capaciteit van mensen en middelen. Om de (digitale) weerbaarheid te vergroten is de gemeente Amersfoort aangesloten bij landelijke ontwikkelingen zoals GGI Veilig, VNG Realisatie en de informatiebeveiligingsdienst (IBD). Ook zijn er initiatieven ontplooid om met collega gemeenten en verbonden partijen kennis te delen, met als doel er samen beter van te worden.

[5] Deze classificaties komen voort uit de richtlijnen van de Informatiebeveiligingsdienst.

4 Organisatie van de informatiebeveiliging

4.1 Verantwoordelijkheden, taken en rollen

Iedereen die werkt binnen de gemeentelijke organisatie heeft een verantwoordelijkheid op het gebied van informatiebeveiliging. In onderstaand figuur is de informatiebeveiligingsorganisatie schematisch weergegeven.



College van B&W

- Stelt de kaders voor informatiebeveiliging vast in het informatiebeveiligingsbeleid op basis van nationale en Europese wet- en regelgeving en nationale normenkaders.[6]

Directie

- Is formeel verantwoordelijk voor de vaststelling en uitvoering van het Informatiebeveiligingsbeleid.
- Stuurt op de risico's;
- Controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden en;
- Evalueert periodiek de beleidskaders en stelt deze waar nodig bij.

CIO-Office

- Adviseert over het informatiebeveiligingsbeleid;
- Houdt toezicht op de werking en naleving van dit beleid, de kaders en richtlijnen.

Concern Information Security Officer (CISO)

- Adviseert en bewaakt informatiebeveiliging op strategisch - en tactisch niveau;
- Houdt toezicht op de implementatie van het beleid en het plan en rapporteert zelfstandig aan de directie of de raad;
- Heeft mandaat om maatregelen door te (laten) voeren;
- Geeft in samenwerking met de concern controller opdracht om audits uit te voeren op de informatiebeveiliging;

[6] Zie bijlage II voor een niet limitatieve opsomming van wet- en regelgeving, richtlijnen en normenkaders.

- Wordt op organisatorische en technische aspecten ondersteund door de adviseurs Informatiebeveiliging.

Functionaris Gegevensbescherming (FG)

- Ziet toe op naleving van privacy wetgeving;
- Adviseert over bescherming en borging van een juiste verwerking van persoonsgegevens in werkprocessen conform de wetgeving.

Afdelingsmanager Informatievoorziening (IV)

- Is opdrachtgever van het informatiebeveiligingsbeleid;
- Draagt zorg voor de beveiliging van de informatievoorziening en implementatie van (technische) beveiligingsmaatregelen die voortvloeien uit risicoanalyses en gegevensclassificaties;
- Draagt zorg voor operationele bewaking en monitoring en voor de rapportage daarover;
- Geeft (technisch) beveiligingsadvies aan de afdelingsmanagers;
- Wordt op organisatorische en technische aspecten ondersteund door de adviseurs Informatiebeveiliging.

Afdelingsmanager Interne Dienstverlening en Advies (IDA)

- Stelt het beleid voor fysieke beveiliging op;
- Is verantwoordelijk voor de fysieke beveiliging.

Afdelingsmanager Organisatie & Talentontwikkeling (O&T)

- Is verantwoordelijk voor onder andere het proces instroom, doorstroom, uitstroom.

Afdelingsmanager

- Is eindverantwoordelijk voor de integrale beveiliging van de afdeling en de daarbij behorende informatiesystemen;
- Legt verantwoording af over informatiebeveiliging aan de CISO via de brede management verantwoording;
- Voert risico-analyses uit op basis van de BIO;
- Stuurt op beveiligingsbewustzijn van medewerkers als onderdeel van de gemeente brede bewustwordingscampagne;
- Wijst een sleutelpersoon aan die voldoende tijd krijgt om aan privacy en informatiebeveiliging te besteden namens de afdeling.

Directeur bedrijfsvoering

- Is eindverantwoordelijk voor de integrale beveiliging van de afdeling overstijgende informatiesystemen die betrekking hebben op de bedrijfsvoering.

Adviseur informatiebeveiliging

- Is onderdeel van team informatiebeveiliging;
- Heeft een adviserende rol richting de CISO;
- Stelt het informatiebeveiligingsbeleid, jaarplannen e.d. op en ondersteunt de CISO;
- Ondersteunt en adviseert directie en afdelingsmanagers bij de informatiebeveiliging;
- Ondersteunt bij uitvoeren risico-analyses en andere vraagstukken van afdelingsmanagers;
- Ziet toe op invulling van de technische beveiligingsmaatregelen.

Product Owner (PO) **Team Informatiebeveiliging**

- Zorgt voor een heldere en concrete prioritering van activiteiten;
- Zorgt voor betrokkenheid van stakeholders en draagt zorg voor hun verwachtingen;

- Voert het informatiebeveiligingsbeleid en stemt activiteiten af met de stakeholders op basis van risicomanagement.

Sleutelpersoon Privacy en Informatiebeveiliging

- Is het eerste aanspreekpunt voor medewerkers binnen de afdeling;
- Ondersteunt de afdelingsmanager bij het uitvoeren van taken voor informatiebeveiliging;
- Sluit aan bij gemeente brede overlegvormen met sleutelpersonen van andere afdelingen;

5 Uitzonderingen

Het kan voorkomen dat er niet volledig kan worden voldaan aan het Informatiebeveiligingsbeleid of het onderliggende IT beveiligingsbeleid. Deze uitzonderingen leiden tot een risico en dienen te worden beheerst. Verzoeken voor uitzonderingen worden gemeld bij de adviseur Informatiebeveiliging. De adviseur Informatiebeveiliging zorgt in overleg met de CISO voor inschatting en vastlegging van het risico. Vastlegging vindt plaats in het exceptieregister. Een exceptie is altijd tijdelijk en maximaal 1 jaar. Na één jaar wordt de situatie herzien en kan er eventueel een nieuwe exceptie worden verleent volgens het voorgenoemde proces. De adviseurs informatiebeveiliging monitoren de opvolging.

6 Controle en verantwoording

Het informatiebeveiligingsbeleid is de verantwoordelijkheid van het bestuur van gemeente Amersfoort. De bestuurders en directie zullen volgens de *10 principes voor informatiebeveiliging (Bijlage I)* richting en sturing geven aan het taakveld informatieveiligheid, onder andere door voorbeeldgedrag en het vragen om informatie.

6.1 Oplevering

Het team informatiebeveiliging levert maandelijks de resultaten van de werkzaamheden op aan de diverse stakeholders. Hierbij worden door de Product Owner diverse stakeholders uitgenodigd, waaronder minimaal de toezichthouders en de CIO. Er wordt hier ruimte geboden voor richting en sturing te geven aan het taakveld informatieveiligheid.

6.2 ENSIA

De gemeente verantwoordt zich jaarlijks over informatiebeveiliging via de ENSIA[7]-systematiek. De ENSIA-coördinator zorgt ervoor dat de informatie benodigd voor het beantwoorden van ENSIA vragen wordt opgehaald bij de verantwoordelijke afdelingsmanagers die de benodigde informatie tijdig aanleveren.

Het college stelt een collegeverklaring op als onderdeel van de ENSIA-verantwoording. In deze verklaring geeft het college van B&W aan in welke mate de gemeente voldoet aan de eisen voor informatiebeveiliging en worden eventuele verbetermaatregelen die de gemeente gaat treffen vermeld. Het college informeert de gemeenteraad over de ENSIA verantwoording.

[7] Eenduidige Normatiek Single Information Audit

Bijlage I - 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader [8] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur;
2. Informatiebeveiliging is van iedereen;
3. Informatiebeveiliging is risicomanagement;
4. Risicomanagement is onderdeel van de besluitvorming;
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6. Informatiebeveiliging is een proces;
7. Informatiebeveiliging kost geld;
8. Onzekerheid dient te worden ingecalculeerd;
9. Verbetering komt voort uit leren en ervaring;
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Wanneer er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

[8] Deze principes zijn sinds de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)

Bijlage II - Overzicht BIO normenkader

Het BIO normenkader is onderverdeeld in een aantal aandachtsgebieden, deze zijn hieronder weergegeven.

5. Informatiebeveiligingsbeleid
    a. Aansturing door de directie van de informatiebeveiliging
6. Organiseren van informatiebeveiliging
    a. Interne organisatie
    b. Mobiele apparatuur en telewerken
7. Veilig personeel
    a. Voorafgaand aan het dienstverband
    b. Tijdens het dienstverband
    c. Beëindiging en wijziging van het dienstverband
8. Beheer van bedrijfsmiddelen
    a. Verantwoordelijkheid voor bedrijfsmiddelen
    b. Informatieclassificatie
    c. Behandelen van media
9. Toegangsbeveiliging
    a. Bedrijfseisen voor toegangsbeveiliging
    b. Beheer van toegangsrechten van gebruikers
    c. Verantwoordelijkheden van gebruikers
    d. Toegangsbeveiliging van systeem en toepassing
10. Cryptografie
    a. Crypto grafische maatregelen
11. Fysieke beveiliging en beveiliging van de omgeving
    a. Beveiligde gebieden
    b. Apparatuur
12. Beveiliging bedrijfsvoering
    a. Bedieningsprocedure en verantwoordelijkheden
    b. Bescherming tegen malware
    c. Back-up
    d. Verslaglegging en monitoring
    e. Beheersing van operationele software
    f. Beheer van technische kwetsbaarheden
    g. Overwegingen betreffende audits van informatiesystemen
13. Communicatiebeveiliging
    a. Beheer van netwerkbeveiliging
    b. Informatietransport
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
    a. Beveiligingseisen voor informatiesystemen
    b. Beveiliging in ontwikkelings- en ondersteunende processen
    c. Testgegevens
15. Leveranciersrelaties
    a. Informatiebeveiliging in leveranciersrelaties
    b. Beheer van dienstverlening van leveranciers
16. Beheer van informatiebeveiligingsincidenten
    a. Beheer van informatiebeveiligingsincidenten en -verbeteringen
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
    a. Informatiebeveiliging continuïteit
    b. Redundante componenten
18. Naleving
    a. Naleving van wettelijke en contractuele eisen
    b. Informatiebeveiligingsbeoordelingen

Bijlage III - Relevante wet- en regelgeving, richtlijnen en normenkaders

- Ambtenarenwet
- Algemene Rijksvoorwaarden bij IT-Overeenkomsten (ARBIT2018)
- Algemene Verordening Gegevensbescherming (AVG)
- Algemene wet bestuursrecht
- Archiefwet
- Baseline Informatiebeveiliging Overheid (BIO)
- Beveiligingsvoorschrift Rijksdienst 2013 (BVR 2013)
- Code voor Informatiebeveiliging (ISO 27001:2013 en ISO 27002:2013)
- Comptabiliteitswet
- Cookiewet
- Eenduidige Normatiek Single Information Audit (ENSIA)
- eIDAS-verordening en eHerkenning
- Forum Standaardisatie open standaarden
- Gemeentelijke arbeidsvoorwaarden (CAR-UWO)
- Kader Rijkstoegangsbeleid
- Netwerk- en informatieveiligheid richtlijn (NIB-richtlijn)
- Norm ICT-beveiligingsassessments DigiD
- Paspoortuitvoeringsregeling Nederland (PUN)
- Programma van Eisen PKI Overheid
- Registratiewet
- Richtlijnen van het Nationaal Cyber Security Centrum (NCSC)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Uitgangspunten online communicatie rijksambtenaren
- Uitvoeringswet AVG (UAVG)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI:2013)
- Wet Basisregistratie Adressen en Gebouwen (BAG)
- Wet Basisregistratie personen (BRP)
- Wet Computercriminaliteit III
- Wet Elektronisch Bestuurlijk Verkeer (WEBV)
- Wet hergebruik van overheidsinformatie
- Wet Openbaarheid van Bestuur (WOB)
- Wet op de identificatieplicht
- Wet Particuliere Beveiligingsorganisaties en Recherchebureaus (WBPR)
- Wet Politiegegevens (WPG)
- Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI)
- Wet Veiligheidsonderzoeken (WVO)
- Wet Werk en Bijstand

Gemeente Amersfoort

Postadres
Postbus 4000
3800 EA Amersfoort

Bezoekadres
Stadhuisplein 1
3811 LM Amersfoort

t 14033
e info-gemeente@amersfoort.nl
i www.amersfoort.nl