Informatiebeveiligingsbeleid
Gemeente Apeldoorn 2020 - 2024

Colofon

EIGENAAR	AUTEUR(S)
College van B&W	Chantal Meijerink - CISO
TITEL	**VERTROUWELIJKHEID**
Informatiebeveiligingsbeleid Gemeente Apeldoorn	Openbaar
STATUS	**TE REVISEREN VOOR**
Vastgesteld	1 januari 2025
TER VASTSTELLING AANGEBODEN OP	
Datum : December 2023 Functie : Burgemeester en Wethouders van de gemeente Apeldoorn	

Versiegeschiedenis

VERSIE	REDEN WIJZIGING	DATUM	STATUS	SCHRIJVER
1.0	Status wijziging	15-12-2014	Vastgesteld	College van B en W
1.5	Status wijziging	20-12-2017	Vastgesteld	College van B en W
1.7	Status wijziging na besluit B&W op 3 maart 2020	05-03-2020	Vastgesteld	Chantal Meijerink
1.8	Geldigheid verlengd tot 31 december 2023	13-01-2023	Vastgesteld	Chantal Meijerink
1.9	Geldigheid verlengd tot 31 december 2024	December 2023	Vastgesteld	Chantal Meijerink

Inhoud

1 Algemeen

1.1 Inleiding

Informatiebeveiliging is een belangrijke pijler onder de betrouwbare dienstverlening die de gemeente Apeldoorn levert. Aspecten als een hoge beschikbaarheid, het correct verstrekken, beheren en verwerken van informatie en het beschermen van vertrouwelijke (persoons)gegevens staan nadrukkelijk aan de basis van onze dienstverlening.

De gemeente Apeldoorn wil aantoonbaar in control zijn ten aanzien van informatiebeveiliging. De gemeente volgt hierbij de internationaal erkende ISO 27001 standaard voor informatiebeveiliging voor het vormgeven van het informatiebeveiligingsproces. Als baseline voor het treffen van beveiligingsmaatregelen volgt de gemeente de Baseline Informatiebeveiliging Overheid (BIO), die gebaseerd is op de ISO 27002. Deze BIO is per 1 januari 2020 voor alle overheidsorganisaties verplicht. Daarnaast volgt de gemeente het ENSIA verantwoordingstraject en legt daarin zowel horizontaal als verticaal verantwoording af over informatiebeveiliging.

Een aantal (technologische) ontwikkelingen zorgt voor blijvende uitdagingen qua informatiebeveiliging, waaronder de veilige uitwisseling van (persoons)informatie tussen organisaties (al dan niet in samenwerkingsverbanden), de groeiende inzet van cloud computing, werken met mobiele apparaten en de groei van beschikbare data en de inzet daarvan in diverse processen, waaronder het DataLab. Om deze ontwikkelingen en mogelijke nieuwe risico's en bedreigingen adequaat het hoofd te kunnen bieden, ligt de nadruk in de komende jaren op het verder professionaliseren van het informatiebeveiligingsproces en het meer risico gebaseerd aanpakken van informatiebeveiligingsvraagstukken.

Dit beleidsdocument geeft richting aan deze verdere professionalisering van het informatiebeveiligingsproces binnen de gemeente Apeldoorn. In het Jaarplan Informatiebeveiliging worden telkens per jaar de concrete activiteiten benoemd die nodig zijn om dit beleid te implementeren.

1.2 Belang en doelstelling van informatiebeveiliging

Informatie is een bedrijfsmiddel dat net als alle andere bedrijfsmiddelen waarde heeft en daarom op passende wijze moet worden beschermd. Informatiebeveiliging is de bescherming van informatie tegen een breed scala van bedreigingen, zowel dreigingen van buitenaf, denk aan bijvoorbeeld een hackaanval vanaf het internet, als tegen dreigingen van binnen uit de organisatie, zoals bijvoorbeeld fraude door eigen medewerkers. Dit informatiebeveiligingsbeleid geldt voor alle vormen van informatie: op papier, elektronisch en mondeling.

Informatiebeveiliging is ondersteunend aan de strategische doelstellingen van de gemeente Apeldoorn. Als belangrijkste doelstelling geldt dan ook voor informatiebeveiliging dat de gemeente Apeldoorn blijvend en aantoonbaar voldoet aan de wettelijke en contractuele verplichtingen op het gebied van informatiebeveiliging en een bijdrage levert aan de continuïteit, betrouwbaarheid en voorspelbaarheid van onze dienstverlening. De gemeente Apeldoorn staat met haar dienstverlening volop in de publieke belangstelling. Het is daarom belangrijk dat maatschappelijke verwachtingen van burgers en andere klanten rond informatiebeveiliging nadrukkelijk meegenomen worden in risicobeheersingsvraagstukken.

1.3 Belangrijke informatiebeveiligingsrisico’s

Ondergenoemde onderwerpen kunnen informatiebeveiligingsrisico’s met zich meebrengen. Deze onderwerpen zijn beheersbaar door een goed ingericht informatiebeveiligingsproces. Onderstaand overzicht van onderwerpen is uiteraard niet uitputtend maar geeft wel een goed beeld van de belangrijkste onderwerpen en ontwikkelingen waar informatiebeveiliging zich op richt, omdat deze onderwerpen en de daaraan verbonden risico’s tot grote schade voor de gemeente kunnen leiden (financieel en/of imago):

Cybersecurity ofwel de weerbaarheid van een organisatie tegen aanvallen vanuit het internet. Het aantal dreigingen vanuit het internet neemt nog altijd toe.[1] Onder ander door het laten uitvoeren van hackerstesten probeert de gemeente kwetsbaarheden tijdig in beeld te krijgen en op te lossen.

Privacy Binnen de gemeente Apeldoorn wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Deze gegevens zijn opgeslagen in meerdere databases (o.a. basisregistraties en Suwinet) en de informatie wordt soms ook nog gecombineerd. In overleg met de Functionaris Gegevensbescherming en de Concern Privacy Officer vindt afstemming plaats over welke data voor welk doel gebruikt mag worden en welke beveiligingsmaatregelen nodig zijn om aan de privacywetgeving te kunnen voldoen.

Cloudcomputing Cloudcomputing is het via internet op aanvraag afnemen van standaard diensten op het gebied van hardware en/of software. De gemeente Apeldoorn maakt steeds meer gebruik van cloudcomputing, bijvoorbeeld de overstap de komende jaren naar MS Office 365 voor de kantoorautomatiseringsomgeving. De gemeente blijft echter eindverantwoordelijk voor een goede informatiebeveiliging, ook als de dienstverlening in de praktijk door een derde partij geleverd wordt. Het is daarom belangrijk bij uitbesteding goede afspraken te maken over informatiebeveiliging en de controle op die afspraken. Bij grote aanbieders van cloudcomputing (bv. Microsoft) is het niet altijd mogelijk om met de leverancier specifieke afspraken over informatiebeveiliging te maken en kunnen er dus extra beveiligingsrisico's kleven aan het gebruik van clouddiensten. Deze dienen per uitbesteding goed te worden afgewogen.

Mobiel werken Het werken met laptops, tablets, mobiele telefoons en andere mobiele apparaten betekent dat er goed bekeken moet worden welke informatie van de gemeente zich waar bevindt en welke beveiliging nodig is om de informatie op de mobiele apparaten voldoende af te schermen.

Data-integriteit Data-integriteit betreft de mate waarin informatie juist is. Op basis van informatie bij de gemeente worden besluiten genomen die voor burgers vergaande gevolgen kunnen hebben, bijvoorbeeld het recht hebben op uitkeringen. Ook wijzigen wij als gemeente informatie die ook door andere overheidsorganisaties gebruikt wordt, dit geldt bijvoorbeeld bij de basisregistraties. Zowel onze klanten als onze ketenpartners moeten uit kunnen gaan van een hoge kwaliteit van onze informatie. Maar ook andere informatie, bijvoorbeeld interne financiële en managementinformatie, dient een hoge mate van betrouwbaarheid te hebben. Door middel van onder meer het beperken van rechten om data te mogen wijzigen en (geautomatiseerde) controles op de kwaliteit van de informatie houden wij de integriteit van de data op het afgesproken niveau.

Bedrijfscontinuïteit Verstoringen in de dienstverlening kunnen direct voelbaar zijn voor onze burgers en andere klanten. Een hoge mate van beschikbaarheid is daarom essentieel voor veel van onze diensten. Vanuit informatiebeveiliging worden passende maatregelen geïmplementeerd om verstoringen te voorkomen, te beperken of snel te kunnen verhelpen.

1.4 Kaders en uitgangspunten voor informatiebeveiliging

Om risico's met betrekking tot informatiebeveiliging beheersbaar te maken gelden bij de gemeente Apeldoorn de volgende kaders en uitgangspunten:

1. Het primaire uitgangspunt voor informatiebeveiliging is risicomanagement, waarbij op basis van een inventarisatie van bedreigingen, kansen en impact de risico's periodiek worden afgewogen.
2. Informatiebeveiliging draagt bij aan het verminderen van de bedrijfsrisico's die een bedreiging vormen voor de strategische doelstellingen van de gemeente Apeldoorn en de uitvoering van haar wettelijke taken. Veilig faciliteren is het uitgangspunt en risico's worden zorgvuldig afgewogen en restrisico's expliciet aanvaard.
3. Het proces en de maatregelen die voortvloeien uit het informatiebeveiligingsbeleid leveren een bijdrage aan de beschikbaarheid, de integriteit en de vertrouwelijkheid van de dienstverlening van de gemeente Apeldoorn. Dit alles op een zo efficiënt en effectief mogelijke wijze.
4. De gemeente Apeldoorn wil aantoonbaar voldoen aan de internationale standaard voor informatiebeveiliging, de ISO 27001 norm, om richting ketenpartners (in bijvoorbeeld

[1] Zie ook het 'Cybersecuritybeeld Nederland 2019' uitgegeven door het Nationaal Cyber Security Centrum en het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020.

samenwerkingsverbanden), burgers en klanten te kunnen aantonen dat wij onze informatiebeveiliging op orde hebben. De normen uit de ISO 27001 gelden als baseline voor het informatiebeveiligingsproces.

5. Als baseline voor het treffen van beveiligingsmaatregelen volgt de gemeente de Baseline Informatiebeveiliging Overheid (BIO), die gebaseerd is op de ISO 27002. Deze BIO is per 1 januari 2020 voor alle overheidsorganisaties verplicht. Van deze normenset wordt alleen onderbouwd afgeweken.
6. De gemeente voldoet aan de beveiligingsvoorschriften zoals die zijn opgenomen in voor de gemeente relevante wetgeving, zoals in ieder geval de wetgeving betreffende de BRP, PUN, SUWI, BGT, BRO en BAG[2], maar ook de AVG, de Archiefwet en de Wet openbaarheid van bestuur (Wob);
7. De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Via het ENSIA verantwoordingstraject legt de gemeente zowel horizontaal als verticaal verantwoording af over informatiebeveiliging.
8. Het 'Plan-Do-Check-Act' (PDCA)-model wordt gehanteerd om het informatiebeveiligingsproces vorm te geven en te verbeteren.
9. Informatiebeveiliging vindt op een integrale wijze plaats. Dit betekent dat maatregelen met betrekking tot de fysieke, personele, IT en juridische aspecten van informatiebeveiliging in hun onderlinge samenhang beoordeeld worden.
10. Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement met het College van B&W als eindverantwoordelijke. Alle verantwoordelijkheden voor activiteiten in het informatiebeveiligingsproces zijn duidelijk belegd en afgebakend.
11. Kennis en expertise zijn essentieel voor een toekomst vaste informatiebeveiliging en zijn door middel van (individuele) opleidingen en voorlichtingscampagnes geborgd.
12. Informatiebeveiliging heeft een relatie met een aantal andere aandachtsgebieden binnen de gemeente Apeldoorn en onderlinge afstemming en samenwerking op deze gebieden is daarom essentieel. Het gaat dan, onder andere, om de volgende aandachtsgebieden: risicomanagement, privacy, informatiebeheer, procesfraude, bedrijfscontinuïteit en de IT(IL)-Service processen.

1.5 Informatiebeveiliging bij de gemeente Apeldoorn in relatie tot onze omgeving

Naast de uitvoering van onze (wettelijke) taken en verantwoordelijkheden voor onze eigen burgers, neemt de gemeente Apeldoorn ook deel aan diverse samenwerkingsverbanden tussen gemeenten of voert de gemeente (wettelijke) taken uit voor andere gemeenten. Daarnaast zijn er ook nog een aantal samenwerkingsverbanden met andere (overheids)organisaties.

Als het gaat om informatiebeveiliging is het belangrijk dat bij samenwerking goed wordt vastgelegd wie welke verantwoordelijkheden heeft en op welke wijze over de uitvoering daarvan aan elkaar gerapporteerd wordt.

1.6 Vervlechting informatiebeveiliging en bescherming persoonsgegevens

Bescherming van de persoonlijke levenssfeer is een fundamenteel recht dat adequaat beschermd moet worden. Een boodschap die in de Europese privacy wetgeving (AVG) duidelijk verwoord is.

Bescherming van persoonsgegevens steunt voor een belangrijk deel op een goede inrichting van informatiebeveiliging in een organisatie. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen en een steeds meer digitale overheid stellen steeds weer andere eisen aan de bescherming van gegevens en privacy. Passende beveiliging van de verwerking van persoonsgegevens is expliciet benoemd in de Europese verordening (Art 32 AVG). Aan het niet goed beveiligen van persoonsgegevens zijn zelfs

[2] BRP staat voor Basisregistratie Personen, PUN staat voor Paspoort uitvoeringsregeling Nederland, SUWI staat voor Wet structuur uitvoeringsorganisatie werk en inkomen en BAG staat voor Basisregistratie adressen en gebouwen.

potentieel forse boetes verbonden. Deze wettelijke verankering om de verwerking van persoonsgegevens te beveiligen zorgt voor een nog grotere vervlechting van de vakgebieden privacy en informatiebeveiliging.

1.7 Reikwijdte, goedkeuring en beheer van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid geldt voor alle diensten en processen die onder de verantwoordelijkheid van de gemeente Apeldoorn plaatsvinden. Het informatiebeveiligingsbeleid is ook van toepassing op diensten die door de gemeente Apeldoorn uitbesteed zijn aan derden. Bij uitbesteding van diensten dienen hierover dan ook afspraken gemaakt te worden met de leveranciers.

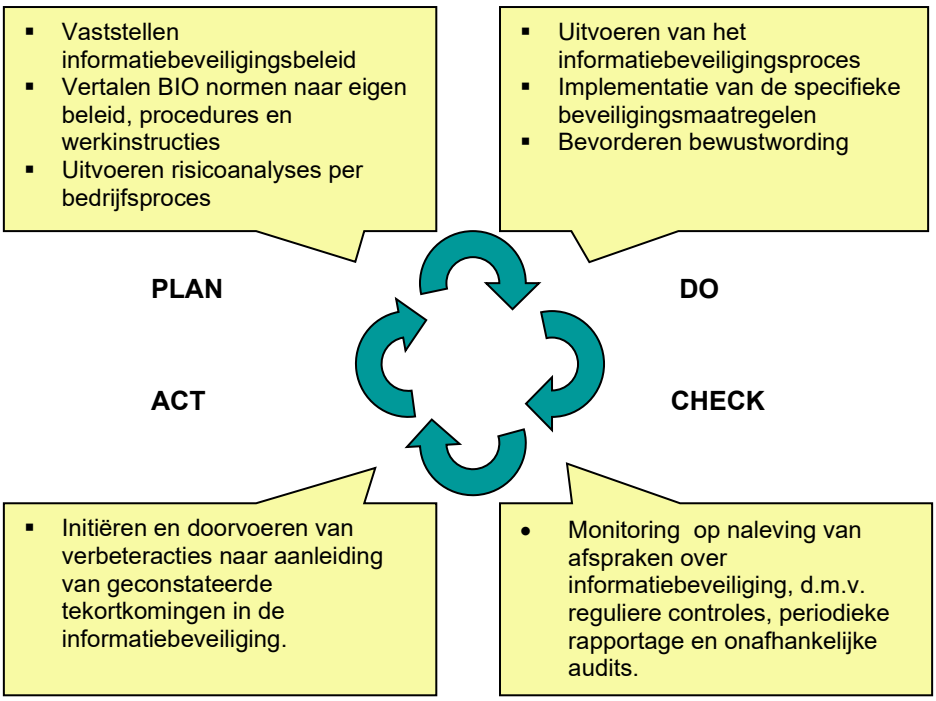
Het informatiebeveiligingsbeleid wordt vastgesteld door het college van Burgemeester en Wethouders en beheerd door de Concern Information Security Officer (CISO). Het beleid wordt 3-jaarlijks (of eerder bij grote wijzigingen) getoetst op actualiteit en indien nodig geüpdatet.

NB. In tegenstelling tot de vorige versie van het informatiebeveiligingsbeleid beschrijft dit beleid nadrukkelijk op strategische niveau de inrichting van het beveiligingsproces. Uitwerking op tactisch niveau van maatregelen vindt plaats in aparte thema gerichte documenten. Nog niet alle onderwerpen zijn uitgewerkt in aparte documenten. Voor die onderwerpen geldt dat de tactische uitwerking zoals opgenomen in het Informatiebeveiligingsbeleid versie 1.5 nog van kracht is totdat het onderwerp in een meer recent document is uitgewerkt.

2 Het informatiebeveiligingsproces

2.1 Het informatiebeveiligingsproces op basis van het PDCA-model

Door informatiebeveiligingsrisico's continu te monitoren is het mogelijk het niveau van informatiebeveiliging op het gewenste en benodigde peil te houden. Waar nodig kan dan ook tijdig bijgestuurd worden. Het informatiebeveiligingsproces is daarvoor ingericht op basis van het Plan-Do-Check-Act model.



Informatiebeveiliging is pas succesvol doorgevoerd in de organisatie wanneer álle medewerkers zorgdragen dat risico's worden vastgesteld en gemeld. Op basis van het informatiebeveiligingsbeleid worden voor risico's passende informatiebeveiligingsmaatregelen geselecteerd (Plan), worden de maatregelen uitgevoerd (Do), wordt periodiek vastgesteld of deze maatregelen nog effectief zijn (Check) en worden – indien nodig -verbeteracties uitgevoerd om tekortkomingen te adresseren (Act).

In de praktijk is er vanzelfsprekend geen sprake van het eenmalig doorlopen van deze PDCA cyclus, maar loopt een aantal cycli door elkaar heen op ook nog eens verschillende besturingsniveaus, namelijk op strategisch, tactisch en operationeel niveau. Aangezien het goed verlopen van het gehele informatiebeveiligingsproces van de gemeente Apeldoorn brede verantwoordelijkheid is, wordt het totale proces bewaakt en gecoördineerd door de Concern Information Security Officer.

2.2 Training en bewustwording

Gedrag is een belangrijke factor bij beveiligingsvraagstukken. De steeds veranderende omgeving en technische hulpmiddelen verlangen dat medewerkers zich bewust zijn van de kansen en risico's van het werken met informatie. Het instellen van regels alleen is in de praktijk onvoldoende. Steeds meer zal de nadruk liggen op het beïnvloeden van het gedrag van medewerkers door bewustwording en het samen vaststellen van de risico's en maatregelen die nodig zijn om deze risico's tot een aanvaardbaar niveau terug te dringen.

Een van de uitgangspunten van de gemeente Apeldoorn bij informatiebeveiliging is dat wordt uitgegaan van vertrouwen. Vertrouwen op de professionaliteit en deskundigheid van de medewerkers en het geven

van vrijheid, handelingsruimte en verantwoordelijkheid binnen de vastgesteld kaders. Dit wordt geborgd in goede afspraken en het duidelijk vastleggen van verantwoordelijkheden. Informatiebeveiliging is een lijnverantwoordelijkheid en het zijn dan ook de lijnmanagers die een grote rol spelen bij het onder de aandacht brengen van het onderwerp informatiebeveiliging in het dagelijks werk van hun medewerkers en waar nodig in overleg met de medewerkers zorgen voor passende opleidingen en scholing.

Gemeentebrede communicatie over informatiebeveiliging is belegd bij de CISO, die dit afstemt met de afdeling Communicatie. Jaarlijks wordt hiervoor een communicatieplan opgesteld, waarin ook de communicatie activiteiten zijn opgenomen die in het kader van privacy worden uitgevoerd.

2.3 Directiebeoordeling

Minimaal één keer per jaar beoordeelt de directie of het informatiebeveiligingsproces (het ISMS) nog geschikt, passend en doeltreffend is. Tijdens deze directiebeoordeling wordt ook afgewogen of er verbetermogelijkheden zijn en of er een noodzaak is om wijzigingen aan te brengen in de beveiligingsaanpak, met inbegrip van het informatiebeveiligingsbeleid en de beheerdoelstellingen. De CISO bereidt deze directiebeoordeling voor en verzorgt de verslaglegging.

Bij de directiebeoordeling worden in ieder geval de volgende punten behandeld:

1. De status van acties uit voorgaande directiebeoordelingen;
2. Wijzigingen in externe en interne onderwerpen die relevant zijn voor het informatiebeveiligingsproces;
3. Analyse en beoordeling van de informatiebeveiligingsprestaties, met inbegrip van trends in:
    a. Afwijkingen en corrigerende maatregelen;
    b. Resultaten van monitoren en meten;
    c. Auditresultaten;
4. Het voldoen aan de informatiebeveiligingsdoelstellingen;
5. Feedback van belanghebbenden;
6. Resultaten van risicobeoordeling en de status van de opvolging van verbeteracties; en
7. Kansen voor continue verbetering.

3 Organisatie, taken en verantwoordelijkheden van informatiebeveiliging

Dit hoofdstuk beschrijft 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, Security Officers) 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.

Het is belangrijk dat verantwoordelijkheden met betrekking tot informatiebeveiliging helder belegd zijn om ervoor te zorgen dat leidinggevenden en medewerkers zich verantwoordelijk voelen voor het melden van risico's en waar nodig tot het uitvoeren van verbeteracties om risico's tot een acceptabel niveau terug te brengen.

3.1 College van Burgemeester en Wethouders

Het College van B&W is eindverantwoordelijk voor informatiebeveiliging en stelt het informatiebeveiligingsbeleid van de gemeente vast. De uitvoering hiervan wordt gedelegeerd aan de directieraad. Het college van B&W informeert de gemeenteraad over informatiebeveiliging. Binnen het college van B&W valt informatiebeveiliging onder de portefeuille van een van de portefeuillehouders. De directieraad adviseert het college van B&W formeel over het vast te stellen beleid.

3.2 De directie

De directieraad geeft sturing aan de uitvoering van het informatiebeveiligingsbeleid en ziet er op toe dat naleving van dit beleid plaatsvindt. De directie wordt hierin ondersteund door de CISO.

De directie zorgt

- dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager;
- dat de afdelingsmanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust;
- 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.
- dit strategisch informatiebeleid wordt uitgewerkt in een aantal tactische documenten over informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente.

De directie wordt periodiek door het lijnmanagement en de CISO geïnformeerd over aanwezige beveiligingsrisico's en gebruikt deze stuurinformatie om te beoordelen of het management zijn verantwoordelijkheden neemt.

3.3 Lijnmanagement

Informatiebeveiliging valt onder de verantwoordelijkheden van alle afdelingsmanagers. Om deze verantwoordelijkheid waar te maken worden zij ondersteund vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, de bijbehorende uitvoerende werkzaamheden wel.

Alle processen, systemen, data, applicaties hebben altijd minimaal één afdelingsmanager als eigenaar; er moet dus altijd iemand verantwoordelijk zijn. Afdelingsmanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten.

Van de leidinggevende wordt verwacht dat hij/zij:

- het informatiebeveiligingsbeleid, de richtlijnen en procedures volgt en uitdraagt en een doorvertaling maakt voor de eigen afdeling;
- monitort in hoeverre de informatiebeveiligingsrichtlijnen binnen de eigen scope van verantwoordelijkheid worden nageleefd en waar nodig bijstuurt;
- risico's m.b.t. informatiebeveiliging identificeert, per risico een afweging maakt in hoeverre het risico valt binnen de risicobereidheid van gemeente Apeldoorn en waar nodig maatregelen treft om de risico's binnen de risicobereidheid te laten vallen;
- voor diensten die onder de verantwoordelijkheid van de afdeling vallen een eigenaar aanstelt die er voor verantwoordelijk is dat voor die dienst de informatiebeveiligingsrisico's in kaart zijn gebracht, passende maatregelen zijn genomen om risico's te beheersen en monitort op de effectiviteit van de genomen maatregelen.
- er voor zorgt dat zijn/haar medewerkers over de juiste autorisaties beschikken bij indiensttreding en de autorisaties worden ingetrokken bij vertrek of, waar nodig, bij wijziging van functie en/of rol;
- verantwoording aflegt aan de directie over de uitvoering van bovenstaande taken en verantwoordelijkheden.

3.4 Medewerkers

Het is de verantwoordelijkheid van elke medewerker om zich aan het informatiebeveiligingsbeleid te houden en een actieve rol te spelen in het beschermen van de informatie die onder de verantwoordelijkheid van de gemeente Apeldoorn valt. Dit geldt ook voor de door de gemeente ingehuurde medewerkers. Medewerkers hebben de verantwoordelijkheid risico's te identificeren en te melden bij het Servicepunt en/of de leidinggevende.

3.5 Specifieke rollen

Concern Information Security Officer (CISO)

De CISO fungeert als een programmamanager informatiebeveiliging die overzicht houdt over de concernbrede informatiebeveiliging. De CISO adviseert over en ontwikkelt beleid op meerdere complexe en brede vakgebieden op concern managementniveau. Hij zorgt voor organisatiebrede afstemming en samenhang ten aanzien van vraagstukken en processen die strategisch dan wel tactisch van aard zijn

De CISO[3]:

- stelt het strategisch informatiebeveiligingsbeleid op en heeft dit beleid in beheer;
- werkt samen met de ISO's het strategisch beleid uit in een aantal tactische beleidsdocumenten over beveiligingsonderwerpen;
- stelt de classificatiemethodiek vast ten behoeve van het vaststellen van het gepaste niveau voor beschikbaarheid, integriteit en vertrouwelijkheid;
- adviseert gevraagd en ongevraagd bij (1) het beoordelen van informatiebeveiligingsrisico's en (2) het implementeren van adequate informatiebeveiligingsmaatregelen in processen en systemen om deze risico's te beheersen;
- bevordert het informatiebeveiligingsbewustzijn binnen de gehele organisatie;
- beheert het risicoregister voor beveiligingsrisico's;
- rapporteert eens per kwartaal aan de directie en het lijnmanagement over de stand van zaken met betrekking tot informatiebeveiliging via de bedrijfsvoeringsrapportage;

[3] De opsomming van taken en verantwoordelijkheden bij de CISO en ISO in dit beleidsdocument is een selectie uit het totale overzicht zoals opgenomen in de functiebeschrijvingen van beide functies.

- stuurt functioneel de ISO's aan en bewaakt dat alle activiteiten in het kader van informatiebeveiliging een samenhangend geheel vormen;
- zorgt voor afstemming van informatiebeveiliging met andere relevante vakgebieden binnen de gemeente;
- onderhoudt contacten buiten de gemeente met relevante organisaties.

Information Security Officer (ISO)

De ISO heeft specifieke inhoudelijke kennis van (een deel van) de uitvoeringsprocessen binnen de gemeente en ondersteunt de proceseigenaar bij het uitvoeren van de risicoafweging en het bepalen van beveiligingsmaatregelen. De ISO ondersteunt de CISO bij de uitvoering van informatiebeveiliging op tactisch en operationeel niveau.

De ISO:

- werkt samen met de CISO het strategisch beleid uit naar tactisch beleid en vertaalt dat naar operationeel beleid en een wijze voor implementatie.
- stimuleert informatiebeveiligingsbewustzijn en creëert draagvlak voor beleid en te treffen maatregelen op het gebied van informatiebeveiliging.
- stemt informatiebeveiliging af met projecten binnen de organisatie en vertaalt technische maatregelen naar de taal van de business.
- signaleert informatiebeveiligingsrisico´s, verbeter- en/of knelpunten, verricht intern onderzoek en rapporteert en/of adviseert daarover.
- adviseert het (lijn)management, gevraagd en ongevraagd, bij de uitwerking van het informatiebeveiligingsbeleid voor hun verantwoordelijkheidsgebieden en bij de implementatie van maatregelen en/of beveiligingsplannen.
- voert risicoanalyses, kwetsbaarheidanalyses en beveiligingsaudits uit (en/of coördineert), voedt het risicoregister, stelt risicoacceptaties op, presenteert analyses, conclusies en advies en bewaakt voortgang en opvolging.
- toetst en evalueert de werking en naleving van (beveiligings)beleid, kaders, richtlijnen en regelgeving.
- coördineert en adviseert bij beveiligingsincidenten.

4 Risicoanalyse en classificatie

Een belangrijk deel van het informatiebeveiligingsproces betreft het uitvoeren van risicoanalyses om het risicoprofiel van een dienst of bedrijfsproces te bepalen. Op basis van het risicoprofiel kunnen vervolgens het gewenste beveiligingsniveau en de daarbij horende (aanvullende) maatregelen vastgesteld worden.

4.1 Risicogebaseerd werken

Binnen het vakgebied informatiebeveiliging is inmiddels breed geaccepteerd dat het niet mogelijk is een organisatie voor de volle honderd procent te beschermen tegen alle dreigingen, onder meer doordat de technologische ontwikkelingen elkaar tegenwoordig snel opvolgen en mogelijke aanvallers over vergaande technische kennis en soms ook financiële middelen beschikken. De gemeente Apeldoorn streeft dan ook naar een optimale beveiliging, waarbij risico's en de kosten van maatregelen tegen elkaar worden afgewogen. Restrisico's die niet door maatregelen worden afgedekt, worden expliciet door de eigenaar van het betreffende informatiesysteem aanvaard. Wanneer een restrisico ook andere informatiesystemen uit kritische bedrijfsprocessen kan raken of strategische doelstellingen van de gemeente Apeldoorn, dan dient een restrisico door de directie te worden geaccepteerd. Omdat niet elk risico door middel van maatregelen is af te dekken, is het belangrijk dat de gemeente Apeldoorn het informatiebeveiligingsproces zodanig heeft ingericht dat het in staat is incidenten snel te onderkennen en er adequaat op te reageren.

4.2 Basisbeveiligingsniveaus

Om risicomanagement hanteerbaar en efficiënt te houden, is in de Baseline Informatiebeveiliging Overheid gekozen voor het werken met drie basisbeveiligingsniveaus (BNN's). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap van een betrouwbare overheid?'. BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare bedreigers nodig is. Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. De controls en overheidsmaatregelen die nodig zijn voor dit niveau zijn opgenomen in de Baseline Informatiebeveiliging Overheid (BIO).

4.3 Risicoanalyse en beveiligingsclassificatie per bedrijfsproces

Om per bedrijfsproces inzicht te krijgen in de specifieke aan het proces verbonden risico's wordt voor elk proces of dienst een basis risicoanalyse doorlopen. Hierbij worden het betreffende proces of dienst en de ondersteunende IT-applicaties in kaart gebracht. Daarnaast wordt het proces of dienst beoordeeld op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. De uitkomst hiervan is een beveiligingsclassificatie, de zogenaamde BIV-code (Beschikbaarheid, Integriteit, Vertrouwelijkheid).

Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie:

- **Beschikbaarheid**: hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
- **Integriteit**: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid).
- **Vertrouwelijkheid**: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

Er wordt onderscheid gemaakt in de niveaus Laag, Midden en Hoog. De gemeente Apeldoorn volgt bij het uitvoeren van risicoanalyses de adviezen en daarbij horende sjablonen van de Informatiebeveiligingsdienst van de VNG.

Het toekennen van classificatieniveaus aan data is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke specifieke maatregelen moeten worden genomen. Dit is bijvoorbeeld relevant voor beheerders die lang niet altijd bekend zijn met de inhoud en dus de waarde van data, maar wel worden geacht adequate beschermingsmaatregelen te treffen.

De risicoanalyse wordt uitgevoerd door de eigenaar van een proces of dienst die daarbij ondersteund kan worden door Security management. Voor het uitvoeren van de risicoanalyse en het vaststellen van de beveiligingsclassificatie wordt gebruik gemaakt van de standaard aanpak zoals die is opgenomen in de hiervoor beschikbare sjablonen. Deze sjablonen worden beheerd door Security management.

De risicoanalyse wordt minimaal eens per drie jaar uitgevoerd voor elke dienst of proces. Bij grote wijzigingen is een tussentijdse update van de risicoanalyse verplicht. De uitkomsten van de risicoanalyse, de beveiligingsclassificatie, een overzicht van de te nemen (aanvullende) beveiligingsmaatregelen en de nog openstaande en geaccepteerde risico’s worden vastgelegd per dienst of proces.

5 Naleving en controle op informatiebeveiliging

5.1 Controleframework voor informatiebeveiliging

De gemeente Apeldoorn heeft het informatiebeveiligingsproces zodanig ingericht dat we aantoonbaar en meetbaar in control zijn. De term ‘in control’ betekent dat we de informatiebeveiligingsrisico’s beheersen, wat wil zeggen dat we de risico’s identificeren, mitigeren of accepteren.

Om vast te kunnen stellen in hoeverre we ‘in control’ zijn, wordt periodiek onderzocht in hoeverre afspraken nageleefd worden ten aanzien van:

1. Het informatiebeveiligingsproces en de inrichting daarvan op basis van de plan-do-check-act cirkel.
2. De implementatie van concrete (technische) beveiligingsmaatregelen.

5.2 Interne toetsing

Binnen de gemeente Apeldoorn vindt de volgende toetsing plaats op de naleving van de beveiligingsmaatregelen:

- Tijdens de dagelijkse bedrijfsvoering vinden controles plaats om vast te stellen of er gewerkt wordt volgens de daarover gemaakte afspraken. Deze controles worden uitgevoerd door of onder regie van het lijnmanagement, dat ook sturende maatregelen treft wanneer afspraken niet nageleefd worden;
- De gemeente voert zelf technische security-onderzoeken uit om o.a. vast te stellen of er kwetsbaarheden zijn;
- Jaarlijks voert de CISO een analyse uit om vast te stellen in hoeverre voldaan wordt aan de Baseline Informatiebeveiliging Overheid. De uitkomst van deze analyse is ook input voor het ENSIA verantwoordingstraject;
- De CISO rapporteert per kwartaal via de bedrijfsvoeringsrapportage aan de directie over de stand van zaken met betrekking tot informatiebeveiliging, waaronder geconstateerde risico's boven de vastgestelde risicobereidheid en de voortgang van de verbeteracties om deze risico's te beheersen;
- De afdeling Interne Controle toetst periodiek of het informatiebeveiligingsproces voldoende effectief geïmplementeerd is.

5.3 Externe (onafhankelijke) toetsing

- In het kader van de jaarrekeningcontrole wordt door de externe accountant een aantal maatregelen in relatie tot informatiebeveiliging getoetst.
- In het kader van de ENSIA verantwoording wordt jaarlijks de beveiliging getoetst van de DigiD-aansluitingen en het gebruik van Suwinet door een onafhankelijke auditor.
- Voor de DigiD-aansluitingen die niet gekoppeld zijn aan een SaaS-applicatie laat de gemeente jaarlijks een verplicht security-onderzoek uitvoeren door een onafhankelijke organisatie.