gemeente Heumen

GEMEENTEBLAD

Officiële uitgave van de gemeente Heumen

Nr. 66334

13 februari

2024

Informatiebeveiligingsbeleid 2024-2028

1. Inleiding

In de gemeentelijke organisatie hebben digitalisering en informatisering een grote rol bij het werken met (persoons)informatie. De inwoner mag verwachten dat deze informatie bij de gemeente in goede handen is en dat deze passend wordt beveiligd. We beschikken als organisatie over veel gevoelige gegevens en we worden als gemeente met al onze ketenpartners steeds afhankelijker van goed werkende informatievoorzieningen en -systemen.

Om als gemeente te borgen dat we consistent zijn in het veilig werken met informatie is het van belang een actueel informatiebeveiligingsbeleid te hebben. Dit plan is opgesteld om ondersteuning te bieden aan het College, gemeentesecretaris, management en de algehele organisatie bij de sturing op en het beheer van informatieveiligheid. Met dit document zet de gemeente Heumen een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en borduurt voort op het informatiebeveiligingsbeleid 2020-2023 en de stappen die in de voorgaande jaren zijn gezet.

Dit beleid hangt samen met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen zijn gesteld, zoals de Wet Basisregistratie Personen (Wet BRP), de Algemene Verordening Gegevensbescherming (AVG), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en de Wet open overheid (Woo). Voor bepaalde taken gelden op grond van deze en wet- en regelgeving specifieke beveiligingseisen. Deze worden in aanvullende documenten geformuleerd. Dit beleidsdocument is richtinggevend en kaderstellend en zijn door de gemeente verder uitgewerkt en concreet gemaakt in diverse protocollen, gedragsregels, procedures en werkinstructies op tactisch en operationeel niveau. Ook worden de rollen en verantwoordelijkheden aangaande informatieveiligheid en privacy beschreven.

1.1. Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt het treffen en onderhouden van samenhangende maatregelen verstaan waardoor er bewust en veilig omgegaan wordt met informatie(systemen). Hierdoor wordt betrouwbaarheid van de gemeentelijke processen, gebruikte informatiesystemen en de daarin opgeslagen gegevens aantoonbaar beschermd en geborgd. De maatregelen borgen de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid en in het geval van incidenten de eventuele gevolgschade (impact) van deze incidenten te beperken. Hoe vertrouwelijker informatie is, hoe meer maatregelen er getroffen moeten worden.

Vier kernpunten van informatiebeveiliging zijn:

- **Beschikbaarheid (of continuïteit)**: 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 (juistheid), volledigheid, tijdigheid van informatie en informatieverwerking, oftewel het in overeenstemming zijn van informatie met de werkelijkheid.
- **Vertrouwelijkheid**: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe bevoegd en geautoriseerd zijn.
- **Controleerbaarheid**: waarborgen dat de beoogde toegang tot gegevens en de juiste werking van systemen continu alsook achteraf te controleren is.

Informatiebeveiliging beperkt zich niet alleen tot ICT of technische maatregelen. Het heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties. Belangrijk om te noemen is dat de menselijke factor en hiermee het gedrag een steeds grotere en fundamentele rol speelt in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk.

1.2. Leeswijzer

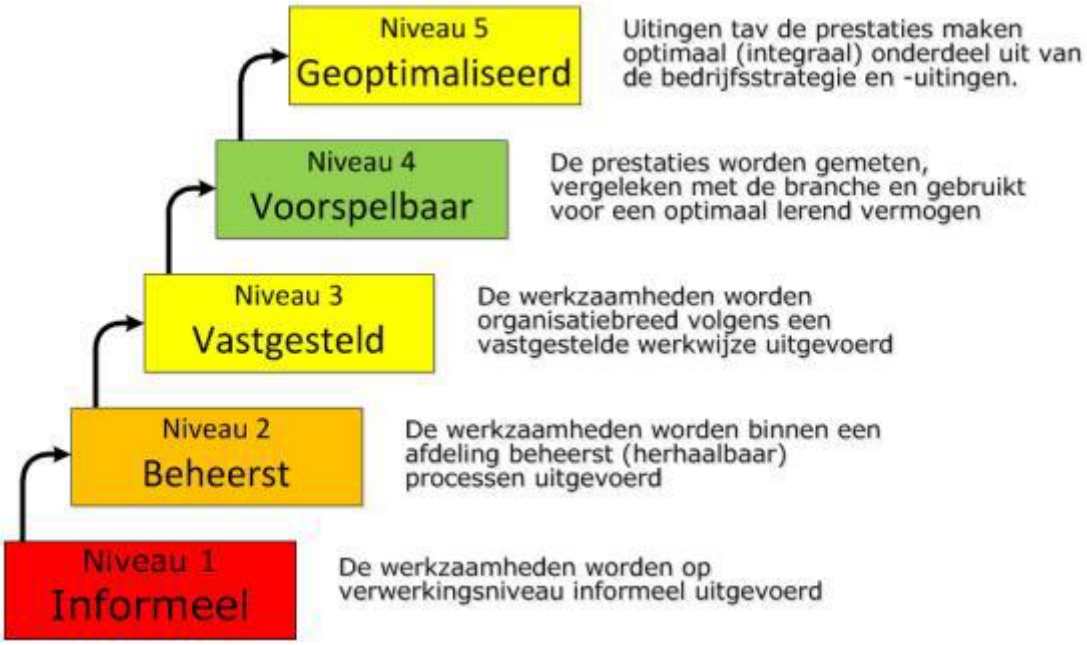
In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie zijn belegd en hoe de verantwoording op informatiebeveiliging plaatsvindt. In het laatste hoofdstuk wordt specifiek aandacht besteed aan de borging van dit informatieveiligheidsbeleid in de organisatie.

2. Strategisch beleid

Dit beleid beschrijft het ambitieniveau aangaande informatieveiligheid in de gemeente Heumen. Er wordt richting gegeven aan de organisatie van informatiebeveiliging binnen de gemeente. Er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en middelen aangegeven waarmee dit beleid wordt vormgegeven.

2.1. Ambitie 2024-2028

De ambitie van de gemeente Heumen is om te zorgen dat de informatieveiligheid van haar informatievoorziening zodanig is ingericht dat de vertrouwelijkheid, integriteit en beschikbaarheid effectief en duurzaam gewaarborgd is. Hierdoor kan de gemeente een ongestoorde dienstverlening verzorgen aan burgers, bedrijven, organisaties, ketenpartners en bezoekers en geeft daarmee tevens continuïteit aan de uitvoering aan haar wettelijke taken.
Om dit te bepalen maken we hierbij gebruik van het BIO-SA model van het Centrum Informatiebeveiliging en Privacybescherming (CIP)[1] dat vijf volwassenheidsniveaus uitdrukt en onderscheid. Op basis van dit model werken we stapsgewijs toe naar een hoger volwassenheidsniveau waarbij uiteindelijk het doel is dat we informatieveiligheid effectief en efficiënt hebben geborgd hebben binnen onze werkprocessen en dit meetbaar is. Het CIP vertaalt de wetgeving op het gebied van informatieveiligheid en privacy naar concrete, hanteerbare normen die duidelijk aangeven wat organisaties dienen te regelen in hun beveiligingsbeleid, de uitvoering en de controle erop.



Afbeelding 1 BIO-SA onderscheidt vijf niveaus (levels) van volwassenheid

We ambiëren een volwassenheidsniveau van informatieveiligheid waarbij we volledig 'in control' zijn. Een organisatie is 'in control' als een organisatie zodanig is ingericht dat er wordt gestuurd op resultaten zodat (indien nodig) bijgestuurd kan worden om zo de doelstellingen te realiseren. Momenteel verschilt het volwassenheidsniveau van de gemeente Heumen per proces, afdeling of systeem. Hierbij heeft de gemeente niet altijd de volledige controle en is zij afhankelijk van de medewerking van ketenpartners. Door de complexiteit van sommige processen is hiervoor het uitgangspunt van de gemeente Heumen om de komende jaren volledig naar niveau 3 toe te groeien. Hiervoor is een gecoördineerde en gestructureerde aanpak noodzakelijk om door te kunnen groeien naar niveau 4/5 zodat we uiteindelijk proactief op ontwikkelingen kunnen anticiperen.

Getroffen maatregelen dienen daarbij continu te worden geëvalueerd en indien nodig geactualiseerd. Daarbij gaat het om intern beleid, normen en procedures, en anderzijds om de technische en organisatorische maatregelen, zoals heldere verantwoordelijkheden en bewustwording van medewerkers.
Hierbij realiseren we ons dat 100% beveiliging tegen cybercriminaliteit altijd een onmogelijke opgave

1) De-16-criteria-van-de-bio-sa-v10.pdf (cip-overheid.nl)

zal blijven. Met het treffen van gerichte maatregelen proberen we beveiligingsincidenten zoveel mogelijk te voorkomen en eventuele gevolgen te minimaliseren.

2.2. Beleidsdoelstellingen

De doelstellingen van dit beleid zijn als volgt:

- Het managen van de informatiebeveiliging;
- Adequate bescherming van bedrijfsmiddelen;
- Het minimaliseren van risico's van menselijk gedrag;
- Het voorkomen van ongeautoriseerde toegang;
- Het beheersen van de toegang tot informatiesystemen;
- Het garanderen van betrouwbare en veilige informatievoorzieningen;
- Het waarborgen van veilige informatiesystemen;
- Het adequaat reageren op incidenten;
- Het beschermen van kritieke bedrijfsprocessen;
- Het beschermen en correct verwerken van persoonsgegevens van inwoners, medewerkers en samenwerkende partijen;
- Het waarborgen van de naleving van dit beleid.

De uitwerking van het beleid in concrete te nemen maatregelen vindt plaats in het jaarplan informatiebeveiliging en privacy. Dit beleid moet volgens de Baseline Informatiebeveiliging Overheid (hierna: BIO) minimaal om de vier jaar opnieuw worden beoordeeld en zo nodig worden bijgesteld.

2.3. Ontwikkelingen en context

2.3.1. De BIO

De basis van dit beleid wordt gevormd door de BIO, deze is opgesteld door de Informatiebeveiligingsdienst (IBD) van de VNG in 2020. De BIO is afgeleid van de internationale informatieveiligheidsnormen NEN-ISO 27001:2017 en 27002:2017. De eerste standaard (ISO27001) is een norm voor de implementatie en planmatige borging van informatieveiligheid binnen de organisatie. De tweede standaard (ISO27002) bevat een verzameling van beveiligingsmaatregelen voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. In de BIO zijn de methodiek en de terminologie specifiek aangepast voor de situatie bij overheden (zowel Rijk, provincie, waterschappen als gemeenten).

De werkwijze van de BIO is gericht op risicomanagement. Risicomanagement is een middel om op een gestructureerde manier risico's in kaart te brengen, te evalueren en – door er proactief mee om te gaan – beter te beheersen. De organisatie inventariseert risico's en diens mogelijke gevolgen en verbindt er maatregelen aan. De BIO gebruikt in dit verband de term controls. Bij alle controls dient bepaald te worden hoe aan de beveiligingsdoelstelling voldaan kan worden. De BIO bestaat uit een baseline met verschillende niveaus van beveiliging. Afhankelijk van uit te voeren risicoanalyses moeten de procesverantwoordelijken, waaronder de gemeentesecretaris en het management per onderdeel uit de BIO kiezen voor bepaalde niveaus van beveiliging met bijbehorende maatregelen. Tevens dienen zij er op toe te zien dat deze maatregelen worden uitgevoerd.

2.3.2. De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De 10 principes voor informatiebeveiliging kan dienen als een kwaliteitsaspect dat in alle processen van de organisatie terugkomt.

De 10 principes voor informatiebeveiliging 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 over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. In de gemeente Heumen zijn deze taken belegd bij het College, de gemeentesecretaris en het management. Zij hebben een rol om de organisatie te faciliteren en het op orde brengen van de informatieveiligheid en privacy bij het bieden van ondersteuning van risicomanagement. Als

er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.3.3. Belangrijkste risico's en ontwikkelingen informatiebeveiliging
Onze gemeente digitaliseert net als de samenleving om ons heen. Zodoende is informatiebeveiliging een onderwerp dat steeds belangrijker wordt. Inwoners en partijen waar wij mee samenwerken willen snel en digitaal geholpen worden maar daarmee nemen moderne en digitale dreigingen alsmaar toe. Het IBD brengt periodiek in kaart wat de actuele, meest belangrijke risico's zijn op het gebied van gemeentelijke informatiebeveiliging. In het *Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023-2024*[2] wordt ingegaan op deze risico's.

De belangrijkste risico's zijn volgens het IBD als volgt:
- **Uitval van dienstverlening en bedrijfsvoering:** als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering.
- **Vertrouwelijke informatie in verkeerde handen:** onterechte toegang tot gevoelige informatie kan uiterst nadelig uitvallen voor inwoners en ondernemers
- **Fouten in de dienstverlening:** informatiebeveiligingsincidenten kunnen leiden tot fouten in dienstverlening. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

Aanvullend op de genoemde risico's valt het IBD in het bijzonder drie soorten dreigingen op:
- **Meer ransomware , met destructievere gevolgen:** aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger.
- **Steeds meer en ernstiger kwetsbaarheden in software:** kwetsbaarheden met een hoge kans op misbruik en ernstige gevolgen komen in de afgelopen jaren relatief steeds vaker voor.
- **Gevaren in ketens uit het zicht:** als gemeente neem je deel aan veel samenwerkingsverbanden. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico's als taken zijn uitbesteed.

Aanvullend op bovengenoemde bekende risico's voeren we als gemeente een eigen registratie waarin incidenten worden vastgelegd. Deze registratie geeft waardevolle informatie om van te leren en zodoende zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van beleid en procedures.

Als gemeente verhogen we onze weerbaarheid door ons te wapenen tegen de toenemende geprofessionaliseerde dreiging. Waarbij ook het softwarelandschap en hiermee onze ICT-infrastructuur aan verandering onderhevig is. Steeds meer applicaties verhuizen van een in huis geïnstalleerde applicatie naar extern gehoste *Software as a Service* (SaaS) oplossingen. Dataverwerking is meer en meer in de Cloud, wat wil zeggen dat applicaties extern bij andere organisaties op de servers staan. Voor ons als gemeente is het belangrijk hier regie op te houden en ervoor te zorgen dat informatieveiligheid altijd vanaf het begin bij vernieuwingen en veranderingen, zowel bij systemen als beleid en processen, meegenomen wordt (*security by design*). Daarnaast controleren en beoordelen we partners actief. Dit geldt ook, zoals het IBD benadrukt, voor ketenpartners waar wij als gemeente mee samenwerken.

Ook de ontwikkeling van het tijd- en plaats onafhankelijk werken heeft voor nieuwe risico's gezorgd. Er worden steeds meer mobiele apparaten gebruikt met gevoelige data en er wordt op verschillende, soms openbare, plekken gewerkt. Dit vergt goede afspraken met onze medewerkers. Afhankelijk van de gevoeligheid van informatie wordt bepaald welke maatregelen moeten worden getroffen wanneer gegevens benaderbaar zijn vanaf een locatie buiten de gebouwen van de gemeente.

Tot slot zijn er meer maatschappelijke ontwikkelingen en innovaties binnen de gemeente en haar ketenpartners. Zo is er steeds meer aandacht voor datagedreven werken, het gebruikmaken van algoritmes en kunstmatige intelligentie. Voor dergelijke ontwikkelingen creëren we een visie om hier goed, efficiënt en veilig mee om te gaan.

2.3.4. Ketenpartners en rol iRvN
De gemeente Heumen neemt deel aan verschillende samenwerkingsverbanden, zoals het Werkbedrijf Rijk van Nijmegen (WBRN) voor de uitvoering van de Participatiewet, het samenwerkingsverband Instituut Bijzonder Onderzoek (IBO) voor de handhaving bij uitkeringsfraude en de Omgeving Dienst Rijk van Nijmegen (ODRN) als uitvoeringsorganisatie voor vergunningen, toezicht en handhaving voor bouw en milieu. Bij deze samenwerkingen is sprake van uitwisseling van informatie, waarvan de gemeente,

2) IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf (informatiebeveiligingsdienst.nl)

eigenaar of beheerder is. Informatiebeveiliging dient onderdeel te zijn van een samenwerkingsovereenkomst en deze mag niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente.

Bijzondere aandacht is er voor de Gemeenschappelijke Regeling ICT Rijk van Nijmegen (iRvN) waarbij de iRvN de ICT (automatisering) voor de gemeente uitvoert. Vanuit die hoedanigheid is iRvN de uitvoerende partij voor een groot gedeelte van de tactische en operationele informatiebeveiligingsrichtlijnen en -maatregelen. Zo neemt iRvN de technische beveiligingsmaatregelen voor onze infrastructuur en verzorgt het ons netwerk (inclusief segmentering) en *back-up en restore* en authenticatie en autorisaties. In de praktijk betekent dit veel afstemming, zowel regionaal tussen de CISO's (Chief Information Security Officer) en de iRvN, maar ook tussen ons als gemeente en iRvN bij bijvoorbeeld nieuwe gegevensverwerkingen. Ook is er formeel een rol voor de iRvN weggelegd bij het bestrijden van een informatiebeveiligingsincident (ICT-crisisprocedure).

IRvN bevindt zich in een continue cyclus waarin verbetertrajecten op het gebied van informatiebeveiliging worden uitgevoerd. Eind 2021 is een onderzoek uitgevoerd naar het beveiligingsniveau van onze infrastructuur. Dit heeft begin 2022 geleid tot het programma om de basis van de informatieveiligheid op orde te houden en stappen te zetten op het gebied van monitoring, detectie en preventie. IRvN werkt toe naar het kunnen afgeven van een volledige TPM (Third Party Memorandum) voor de BIO in 2025 en houdt alle deelnemers op de hoogte van de vorderingen binnen de verbetertrajecten en brengt periodiek verslag uit aan de betrokken functionarissen.

Om de samenhang in informatiebeveiliging tussen de deelnemende gemeenten van iRvN te waarborgen is een CISO-overleg informatiebeveiliging ingesteld. Ook participeert iRvN in allerlei landelijke platforms en onderhoudt o.a. contacten met de Informatiebeveiligingsdienst Gemeenten (IBD) en het NCSC.

2.3.5. Relatie met privacy

Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt en vaak hand in hand gaan. Het zijn twee verschillende begrippen, echter met een gemeenschappelijk raakvlak. Informatiebeveiliging heeft namelijk een bredere scope dan de bescherming van enkel persoonsgegevens.

Informatiebeveiliging draait om de bescherming van alle gevoelige informatie(systemen) tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek-gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn. Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywet. Artikel 32 van de AVG schrijft voor dat:

"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen".

Informatiebeveiliging maakt daarmee een onderdeel uit van de AVG. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Normenkaders als de BIO helpen de gemeente om de risico's goed in te schatten en de benodigde maatregelen te treffen. In de praktijk betekent dit dat de CISO en de Functionaris Gegevensbescherming (FG) nauw samenwerken. Hoe de gemeente omgaat met privacy en de AVG is beschreven in het privacybeleid 2023-2027 van de gemeente Heumen.

2.4. Belangrijkste uitgangspunten en voorwaarden

De belangrijkste uitgangspunten van het beleid zijn:

- Het College van B&W is bestuurlijk eindverantwoordelijk voor de informatiebeveiliging van de gemeente Heumen. Het College stelt het informatiebeveiligingsbeleid vast.
- De uitvoering en handhaving van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Heumen hebben een interne eigenaar die de vertrouwelijkheid bepaalt van de informatie die ze bevatten.
- Informatiebeveiliging is een continu verbeterproces: 'plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- Over de uitvoering van het beleid wordt periodiek gerapporteerd aan College en management en – als onderdeel van de jaarlijkse Planning & Control-cyclus – aan de gemeenteraad. Het managementteam (MT) stelt jaarlijks het informatiebeveiligingsplan vast en zorgt dat acties worden uitgevoerd.

- Maatregelen op het gebied van informatieveiligheid worden getroffen na een zorgvuldige risicoafweging, waarna op basis van de grootste risico's eerst de prioritering wordt gegeven en maatregelen worden getroffen.
- Verantwoord en bewust gedrag van medewerkers is essentieel voor goede informatieveiligheid. Iedere medewerker, zowel vast als tijdelijk, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerd gebruik en bij vermeende inbreuken hiervan melding te maken. De medewerkers die werken met de informatiesystemen van de gemeente worden getraind in het gebruik van beveiligingsprocedures en kennis en bewustzijn van informatiebeveiliging.
- Toegang tot applicaties, waarin gevoelige gegevens worden verwerkt, is beperkt. Toegang tot informatie wordt uitsluitend verleend als die noodzakelijk is voor de uitoefening van de functie (het *need-to-know principe*). Ook vindt periodiek evaluatie plaats van de rechten die zijn uitgegeven.
- Iedere medewerker is individueel identificeerbaar bij het gebruik van ICT-systemen en/of applicaties, waardoor monitoring en controle kunnen worden ingericht. Groepsaccounts zijn niet toegestaan.
- Bij de uitvoering van het informatieveiligheidsbeleid werken we volgens erkende methodieken en architectuur.
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- IRvN is de uitvoerende partij voor (lokale) technische beveiligingsmaatregelen. SaaS leveranciers zijn zelf verantwoordelijk en worden hierop kritisch beoordeeld.

2.5. Bevordering beveiligingsbewustzijn

Informatiebeveiliging gaat over veel meer dan ICT. Uiteindelijk is menselijk gedrag en beveiligingsbewustzijn de belangrijkste factor voor het veilig houden van informatie en de dienstverlening. Vrijwel alle beveiligingsincidenten uit de recente geschiedenis zijn terug te herleiden naar een menselijke fout. Het is noodzakelijk dat alle medewerkers de juiste instelling hebben ten aanzien van informatieveiligheid en privacy en dat het College, de gemeentesecretaris en het management dit actief uitdraagt en stimuleert. Op deze manier wordt het juiste gedrag bevorderd en ontstaat een cultuur waarin men elkaar aanspreekt op fout en goed gedrag. De gemeente faciliteert en stimuleert de verbetering van bewustwording planmatig en structureel door middel van E-learnings, presentaties van deskundigen, en speciale activiteiten zoals een *mysteryguest* en *phishing* campagnes. Het is de verantwoordelijkheid van iedere medewerker om de aangeboden kennis tot zich te nemen en toe te passen.

3. Organisatie en verantwoording

In dit hoofdstuk wordt het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen benoemd met de hieraan verbonden verantwoordelijkheden uiteengezet. Hiermee wordt duidelijk welke taken, verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de gemeente Heumen.

3.1. Rollen en taken

Dit beleid en hiermee informatiebeveiliging is een verantwoordelijkheid van het College van B&W van de gemeente Heumen. De gemeentesecretaris, het College en het management van de gemeente zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging. Met betrekking tot informatiebeveiliging worden in de gemeente Heumen de volgende rollen onderkend. In bijlage 1 is een uitgebreide omschrijving van de rollen en taken te vinden.

De gemeenteraad
De gemeenteraad controleert het College op het naleven en toepassen van wet- en regelgeving op het gebied van informatiebeveiliging.

College van B&W
Het College van Burgemeester en Wethouders (B&W) keurt het beleid formeel goed en draagt zorg voor de naleving van het beleid in de gemeente . Het college stelt de kaders vast voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

Gemeentesecretaris
De ambtelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de gemeentesecretaris. De gemeentesecretaris is daarmee eind verantwoordelijke in de praktijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de (informatie)systemen.

Afdelingshoofd (MT)
Informatiebeveiliging valt onder de verantwoordelijkheid van alle afdelingshoofden die worden ondersteund vanuit de tweede lijn. Uitgangspunt daarbij is dat de lijnmanager verantwoordelijkheid draagt voor zowel de resultaten van het primaire proces als voor de ondersteunende processen.

Applicatiebeheerder
De applicatiebeheerder is voor een specifiek toegewezen applicatie primair verantwoordelijk en aanspreekpunt voor alle activiteiten gericht op de naleving van de maatregelen en procedures binnen de applicatie. Met betrekking tot informatieveiligheid is de belangrijkste taak het correct bijhouden van de autorisaties.

Teams
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot de eigen functie en taken. De teams zijn eigenaar van - en integraal verantwoordelijk voor de (informatie)veiligheid - de informatieprocessen en -systemen binnen de eigen invloedsfeer.

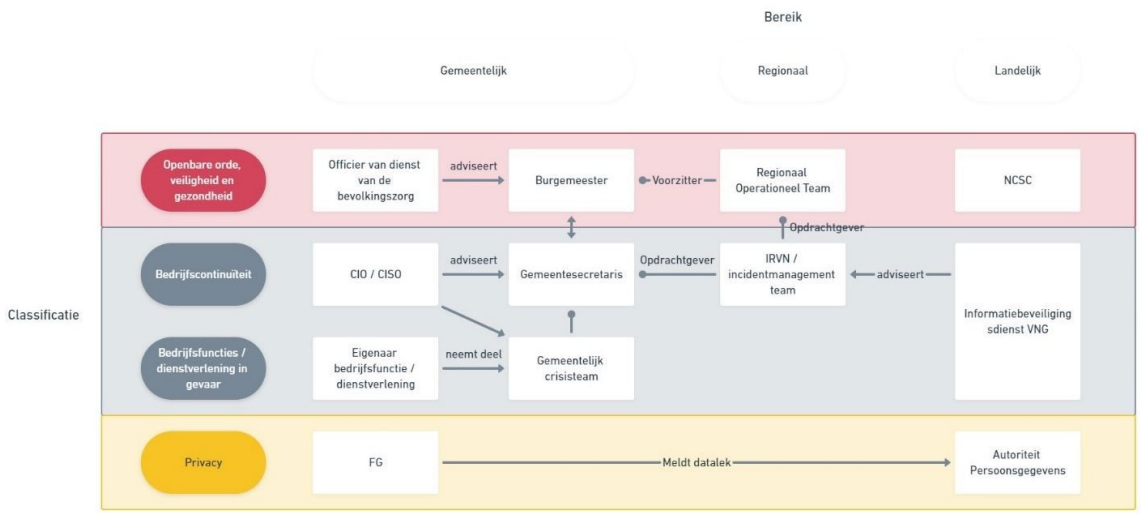
Chief Information Security Officer (CISO)
De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het MT. De CISO is verantwoordelijk voor het voorbereiden en opstellen van het beleid (beleidsvoorbereiding) en coördineert de implementatie van het beleid. De CISO is kortom de beleidsfunctionaris die taken uitvoert op het gebied van informatiebeveiliging en is de spin in het web van de informatiebeveiliging.

Functionaris Gegevensbescherming (FG)
De FG is conform de Algemene Verordening Gegevensbescherming (AVG) de onafhankelijk toezichthouder en adviseur op alle wet- en regelgeving die te maken heeft met het verwerken van persoonsgegevens binnen de gemeente. De FG adviseert rechtstreeks de gemeentesecretaris en de portefeuillehouder. In de praktijk stemmen de CISO en de FG adviezen op elkaar af en werken nauw samen.

Interne controle (auditor)
Team informatiebeveiliging en privacy (CISO/FG) stelt jaarlijks een controleplan op waarmee de interne controle op het functioneren van de beveiligingsorganisatie wordt gecontroleerd. Om te beoordelen of de gemeente Heumen haar informatieveiligheidsbeleid- en doelstellingen behaalt, worden periodieke onafhankelijke audits - waarbij een onafhankelijke deskundige partij een toets uitvoert op de opzet, bestaan en werking van beheersmaatregelen - en controles uitgevoerd. Hiertoe kan een externe (erkende) partij worden ingeschakeld of de eigen afdeling concern control/auditafdeling.

3.2. ICT-crisisbeheersing en samenwerking
Voor interne crisisbeheersing is er een crisisteam geïnstalleerd. Dit crisisteam bestaat in ieder geval uit: de gemeentesecretaris, de CISO en de proceseigenaar of afdelingshoofd. Op basis van de aard van het incident wordt het crisisteam uitgebreid met de PFO/Burgermeester, communicatie en/of de CISO's van de andere mogelijk betrokken deelnemende gemeenten uit de regio. Bij afwezigheid wordt er een plaatsvervanger aangesteld binnen de eigen organisatie en/of kan er een beroep worden gedaan op de expertise vanuit de regio.

In het geval van regionale crisisbeheersing borgt de gemeente Heumen zich middels een mandaatbesluit als deelnemende organisatie binnen de regionale samenwerking tot de afbakening van taken en bevoegdheden van de voorzitter van het regionaal incidentbestrijdingsteam. Dit is vastgelegd in een lokale en regionale ICT-crisis procedure.



Figuur 1 Regionale verdeling verantwoordelijkheden op basis van classificatie en bereik naar interne organisatie.

4. Borging en verantwoording informatiebeveiligingsbeleid

4.1. PDCA-cyclus informatiebeveiliging

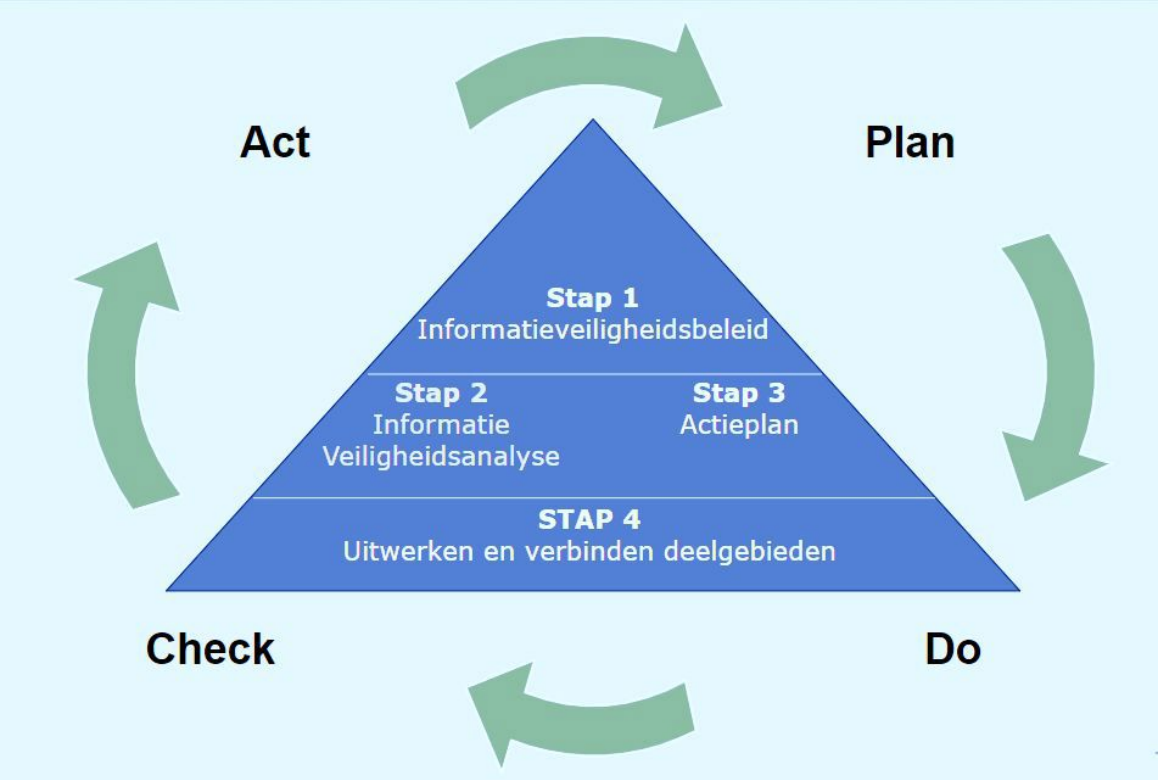
Om de borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren wordt onderstaande Plan, Do, Check, Act (PDCA)-cyclus doorlopen (afbeelding 2). De volgende uitgangspunten worden gehanteerd voor het doorlopen van de PDCA-cyclus en wordt bijgehouden in een Information Security Management System (ISMS).

Stap 1. Informatiebeveiligingsbeleid: actualisering beleid
Dit is een organisatie breed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar, dit wordt ook wel het 'pas toe of leg uit' principe genoemd. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van vier jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats.

Stap 2. Analyse van de informatieveiligheid en privacy: dataclassificatie
Deze stap is gericht op de invoering en begint met een informatieveiligheidsanalyse. Hiertoe wordt allereerst een overzicht opgesteld van gegevensverzamelingen/applicaties in de gemeentelijke organisatie. Deze worden toegewezen aan een eigenaar en na onderzoek geclassificeerd op de risicoklassen beschikbaarheid, integriteit en betrouwbaarheid. Ook wordt daarmee het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld.

Stap 3. Actieplan: jaarplan informatiebeveiliging en privacy
Op basis van de informatieveiligheidsanalyse wordt een actieplan opgesteld, wat de basis is voor het jaarlijkse informatiebeveiliging en privacy plan. De in de analyse geconstateerde risico's worden gewogen waar nodig van maatregelen voorzien. Prioritering van de acties wordt gedaan op basis van de risico's die zijn geconstateerd, de beschikbare tijd, beschikbare middelen en afstemming met betrokkenen. Hierdoor ontstaat een compact actieplan waarmee de gemeente vaststelt welke verbeteracties gedurende het volgende jaar worden uitgevoerd. Dit actieplan vormt een praktische leidraad voor de verbetering en borging van informatieveiligheid in de organisatie en wordt vastgesteld door het managementteam.

Stap 4. Verbindende deelgebieden: technische en organisatorische maatregelen
Stap vier bestaat uit het opleveren van een complete set aan technische en organisatorische maatregelen die gericht zijn op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO, maar ook om applicaties zoals de BRP, SUWI, de BAG, het financiële systeem, of om de primaire processen van de organisatie, ICT-beheerprocessen of de inrichting van de ICT-platformen (iRvN). Dit betreft met name het opstellen en bijstellen van procedures en werkinstructies en het daadwerkelijk implementeren van technische of organisatorische verbeteringen op het gebied van informatieveiligheid.



Afbeelding 2 PDCA-cyclus informatieveiligheid

4.2. Audits (ENSIA) en controle

Om te beoordelen of de organisatie zijn informatiebeveiligingsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke audits en controles uitgevoerd. Bij een audit toetst een onafhankelijke deskundige partij op de opzet, bestaan en werking van beheersmaatregelen. Hiervoor wordt doorgaans een externe partij ingeschakeld. Deze diverse interne en externe audits uitgevoerd bieden input voor het actieplan zoals genoemd onder stap twee van de PDCA-cyclus. Als resultaat van de audit kunnen eventuele zwakheden in de beveiliging ontdekt worden en dit kan tot gevolg hebben dat er aanpassingen noodzakelijk zijn in het beveiligingsbeleid. De gemeente verantwoordt zich over informatiebeveiliging middels de jaarlijks verplichte ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). De ENSIA toets door middel van zelfevaluaties en audits enerzijds de kwaliteit van de basisregistraties en anderzijds de informatiebeveiliging (afbeelding 3).

Naast de ENSIA en overige audits zijn er meer controles. Zo wordt informatiebeveiliging als onderdeel van de accountantscontrole meegenomen, maar kan er ook sprake zijn van een Rekenkameronderzoek. Als onderdeel van de informatiebeveiliging jaarplan worden verschillende controles of onderzoeken uitgevoerd op onderwerpen als autorisatiebeheer en toegangscontrole. Ook controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel en input voor het actieplan. Ten slotte leren we van incidenten door deze zorgvuldig te registreren en te evalueren.

ENSIA	Verantwoording over informatiebeveiliging aan gemeenteraad	Verantwoording aan toezichthouders
Zelfevaluatie	• Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO). • Domeinspecifieke vragenlijsten voor diverse stelsels. • Zelfevaluatie afronden en vastleggen in ENSIA.	Vragenlijsten: • RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). • BKWI: Informatiebeveiliging Suwinet (BIO). • Logius: Informatiebeveiliging DigiD. • DGBRW: Datakwaliteit en -integriteit BAG, BGT en BRO.
Opstellen	• Genereren en opstellen verantwoordingsrapportages. • Audit door gecertificeerde RE-auditor over collegeverklaring Suwinet en DigiD. • Opstellen rapportage ENSIA t.b.v. de gemeenteraad.	Producten: • Collegeverklaring over Suwinet en DigiD. • Rapportage BAG, BGT en BRO door college van B&W. • Uittreksels BRP en Reisdocumenten. • Rapportage ENSIA voor de gemeenteraad.
Verantwoorden	• Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W. • Uploaden en aanleveren verantwoordingsrapportages via ENSIA (Uittreksels BRP en Reisdocumenten verwerken in de rapportages uit de Kwaliteitsmonitor en daar uploaden).	Resultaten: • De toezichthouders BKWI, Logius en DGBRW krijgen via ENSIA de verantwoordingsrapportages aangeleverd. • RvIG krijgt de informatie uit de Uittreksels BRP en Reisdocumenten via de Kwaliteitsmonitor aangeleverd.
Versturen	• Opstellen paragraaf verantwoording informatiebeveiliging voor de paragraaf Bedrijfsvoering in het jaarverslag. • Gemeenteraad neemt kennis van rapportage ENSIA. • College van B&W stelt jaarverslag vast. • Gemeenteraad keurt jaarverslag goed. • Het college van B&W stuurt het gemeentelijk jaarverslag aan de provincie.	• De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd. • De vastgestelde jaarstukken zijn aan de provincie toegestuurd.

Afbeelding 3 Het verantwoordingsproces ENSIA

Bijlage 1 Uitwerking rollen informatiebeveiliging gemeente Heumen

De gemeenteraad

Toetsing en controle: de gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente. Het College legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de raad, door middel van een collegeverklaring/In Control Verklaring (ICV) – waarop door een auditor assurance wordt afgegeven – en daarnaast in het jaarverslag met een passage over informatiebeveiliging in de paragraaf bedrijfsvoering.

College van B&W

Het College van Burgemeester en Wethouders (B&W) keurt het beleid formeel goed en draagt zorg voor de naleving van het beleid in de gemeente. Ook is er een portefeuillehouder ICT vastgesteld die verantwoordelijk is voor informatiebeveiliging.
Het college informeert de Raad over de informatiebeveiliging van de gemeente door een aparte paragraaf op te nemen in de jaarrekening van de gemeente of door het doorgeleiden van een jaarrapportage.

Gemeentesecretaris

De gemeentesecretaris zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De gemeentesecretaris zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De gemeentesecretaris 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 verantwoorden naar de raad. De gemeentesecretaris heeft o.a. de volgende taken en bevoegdheden:

- Het stellen van kaders en het geven van sturing voor de veiligheid van informatie (gewenste niveau van continuïteit en vertrouwelijkheid);
- Het sturen op concern risico's;
- Het periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het (waar mogelijk) inrichten van functiescheiding tussen beleidsbepalende, uitvoerende en controlerende taken met betrekking tot informatiebeveiliging
- Autoriseren procedures en uitvoeringsmaatregelen.

Afdelingshoofd (MT)

De afdelingshoofden Bouwen Milieu en Leefomgeving (BML), Sociale Leefbaarheid (SOLE), Publiekszaken (PUZA), Bedrijfsondersteuning (BEON) en Facilitaire ondersteuning (FAON) zijn verantwoordelijk voor informatiebeveiliging in zijn of haar afdeling. Het afdelingshoofd onderhoudt hiervoor contact met de medewerkers die behoren bij de eigen afdeling en zorgt voor een correcte naleving van het beleid door zijn medewerkers (beleidsuitvoering). De belangrijkste taken en bevoegdheden van het afdelingshoofd, in afstemming met CISO en FG in het kader van informatiebeveiliging zijn:

- Rapporteren aan het college of gemeentesecretaris over de onder hun verantwoordelijkheid tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld;
- Het leveren van input voor nieuwe maatregelen en procedures en het uit laten voeren van maatregelen uit het jaarlijkse informatiebeveiligings- en privacyplan die op de afdeling van toepassing zijn;
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures waarbij er zorgt voor wordt gedragen dat de teams de CISO en de FG tijdig betrekken.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen;
- Het sturen op beveiligings- en privacybewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen

Applicatiebeheerder

Binnen de teams zijn er bepaalde medewerkers, voornamelijk applicatiebeheerders die fungeren als eerste aanspreekpunt voor team informatiebeveiliging en privacy omdat zij proceseigenaar zijn van een brede set informatie, wat aanvullende taken met zich mee brengt qua beheer, de coördinatie en advies ten aanzien van informatiebeveiliging en privacybescherming van specifieke gegevensverzamelingen en specifieke wet- en regelgeving.

Tot de taken en bevoegdheden van elke applicatiebeheerder behoren:

- Controleren, signaleren, rapporteren en aanpassen van de processen en applicaties; Tevens eerste aanspreekpunt.
- Informatiebeveiliging en privacy meenemen in beslissingen over de lopende en nieuwe processen en voorschriften van de applicaties;
- Uitvoering, toezicht en rapportage op de voorbereiding en uitvoering van het beveiligingsbeleid en- plan (en wet- en regelgeving) en hiermee compliance aan het afdelingshoofd en CISO/FG m.b.t. de eigen processen en applicaties.
- Vastleggen en beheren van maatregelen ten behoeve van eigen processen en applicaties in het Information Security Management System (ISMS).
- Opstellen van gebruikersdocumentatie informatiebeveiliging (en configuratie applicatie) zoals handleidingen, procedures, werkwijzen.
- Het classificeren van opgeslagen data in applicaties en gegevensverzamelingen en het opstellen van betrouwbaarheidseisen van applicaties/systemen.
- Beoordelen, toekennen en monitoren van autorisaties aan gebruikers op basis van een vastgesteld proces en met behulp van een autorisatiematrix;
- Toezicht houden dat nieuwe medewerkers worden geïntroduceerd en bekend gemaakt met de beveiligingsprocedures. Inclusief medewerkers aanspreken op de verantwoordelijkheid in hun dagelijkse werkprocessen en hiermee het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen.

We onderscheiden de volgende applicatiebeheerders:

- Applicatiebeheerder fysieke toegang en locatiebeheer: verantwoordelijk voor fysieke beveiliging van - en in - gebouwen en ruimtes binnen de gemeente.
- Beveiligingsbeheerder automatisering ICT Rijk van Nijmegen (iRvN): o.a. verantwoordelijk voor de technische beveiliging en beheer aspecten op het gebied van automatisering, zoals ICT security management, incident- en probleem management. Verzorgt logging, monitoring en rapportage over de automatisering en geeft advies.
- Applicatiebeheerder P&O: verantwoordelijk voor het bijhouden van persoonsgegevens van medewerkers en het in-en uitdiensttredingsproces.
- Applicatiebeheerder financiën: verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures op het gebied van financiële gegevens en alle daaraan gekoppelde registraties. Denk daarbij aan gevoelige informatie van crediteuren en debiteuren.
- Applicatiebeheerder inkomen: verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit de Participatiewet en Basis beveiligingsrichtlijnen SUWI. Denk daarbij aan gevoelige cliëntinformatie op het gebied van werk, uitkeringen en re-integratie.
- Coördinator kernteam: in de gemeente is de coördinator van het kernteam verantwoordelijk voor de beveiliging van de gegevens die verwerkt worden binnen het sociaal team.
- Applicatiebeheerders BAG, BGT en BRO en gegevensbeheer: toezien op naleving van de Wet- en Regelgeving van deze basisregistraties.
- CISO: is verantwoordelijk voor de realisatie van een betrouwbare, veilige en efficiënte inrichting van de informatievoorziening van de gemeente, waarbij rekening wordt gehouden met wet- en regelgeving. Ondersteunt functioneel-, gegevens- en applicatiebeheerders en verzorgt inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.
- Applicatiebeheerder DigiD: een taak die bij de (web)applicatiebeheerder van de DigiD-aansluiting is belegd en verantwoordelijk is voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit de Basis beveiligingsrichtlijnen DigiD, zoals technische maatregelen bij de externe leverancier (infrastructuur, segmentering etc.) en de interne dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer die jaarlijks wordt getoetst (ENSIA). Denk daarbij aan de bescherming van persoonsgegevens, voor zover een softwareleverancier waaraan diensten zijn uitbesteed daar niet voor verantwoordelijk is. Ook rapporteert de beveiligingsbeheerder DigiD hierover periodiek aan het afdelingshoofd Publiekszaken.
- Security Officer Suwinet: De security officer Suwinet is verantwoordelijk voor de beveiliging van Suwinet. De taken en bevoegdheden van de security officer Suwinet zijn:
    - Aanspreekpunt voor Suwinet binnen de gemeente en bevordert en adviseert op het gebied van informatiebeveiliging Suwinet;
    - Bevordert en beheerst beveiligingsprocedures en – maatregelen in het kader van Suwinet, zodanig
    - dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is ingevoerd;
    - Controleert of en in hoeverre beveiligingsmaatregelen en -procedures worden nageleefd en monitort
    - de uitvoering van het opgestelde beleid;
    - Evalueert de uitkomsten en doet voorstellen voor implementatie en aanpassing van plannen op het

- gebied van de beveiliging Suwinet;
- Overlegt met CISO, het afdelingshoofd en de applicatiebeheerder inkomen over informatiebeveiliging en -beheer Suwinet;
- Stelt het informatiebeveiligingsplan Suwinet op en coördineert de periodieke evaluatie;
- Voert jaarlijks een controle uit op de naleving van het informatiebeveiligingsplan Suwinet;
- Rapporteert jaarlijks over het informatiebeveiligingsplan aan het afdelingshoofd;

- Applicatiebeheerder BRP en Reisdocumenten en Rijbewijzen: de applicatiebeheerder BRP en reisdocumenten en rijbewijzen is een taak die bij de afdeling Publiekszaken is belegd en verantwoordelijkheid met zich mee brengt om toe te zien op naleving van de beveiligingsmaatregelen en –procedures op het gebied van Basisregistratie Personen (BRP) en op het treffen van maatregelen om reisdocumenten en rijbewijzen, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreemding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins. Tevens verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations) en voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

Teams
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Onbewust menselijk handelen is de belangrijkste bedreiging voor de gemeentelijke informatievoorziening. Ongewenste, onbewuste acties blijken een groter risico voor de privacy van inwoners en de veiligheid van informatie dan bewuste en gerichte aanvallen. Zij dienen zorgvuldig en gedisciplineerd om te gaan met informatie en (informatie)systemen en zich bewust te zijn van eisen ten aanzien van de betrouwbaarheid, de integriteit en de beschikbaarheid van de informatieprocessen waarbij zij zijn betrokken. Mocht een medewerker iets signaleren m.b.t. informatieveiligheid of privacy neemt diegene contact op met de CISO of FG.

Chief Information Security Officer (CISO)
De CISO is de belangrijkste adviseur op het gebied van informatiebeveiliging. De CISO is verantwoordelijk voor de controle op een juiste uitvoering van het informatiebeveiligingsbeleid, de realisatie van de veiligheidsmaatregelen en de classificatie, coördinatie en escalatie van beveiligingsincidenten. Hieronder valt ook het controleren van autorisatiematrices. De CISO kan hiertoe de interne controle opdracht geven. De CISO is door het college gemandateerd en heeft de volgende taken en bevoegdheden:
- Beleid en coördinatie: het opstellen en actualiseren van het informatiebeveiligingsbeleid; het opstellen van informatiebeveiligingsplannen voor afdelingen of deelgebieden. Het coördineren van de werkzaamheden van collega's, afdelingen en instanties die betrokken zijn bij de uitvoering van het informatiebeveiligingsbeleid en -plan en het ondersteunen van college of gemeentesecretaris en de leidinggevenden met kennis over informatiebeveiliging. Treedt op als coördinator bij een ICT-crisis.
- Controle en registratie: het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid; Het beheersen van de risicoanalyses en toezicht houden op de processen en beveiligingsmaatregelen Het bijhouden van de registratie van informatiebeveiligingsincidenten en het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten. Stelt controleplannen op en voert risicoanalyses en interne audits uit of initieert deze.
- Communicatie en voorlichting: het onderhouden van externe en interne contacten op alle niveaus over informatiebeveiliging en deelname aan overleggen met betrekking tot informatiebeveiliging.
- Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn; Aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatiebeveiliging en contactpersoon van de gemeente voor de Informatie Beveiligingsdienst (IBD).
- Advies en rapportage en uitvoering: het opstellen en uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen, waarbij ook afgestemd wordt met lopende projecten binnen de organisatie. Overleg en rapportage o.a. via de P&C cyclus over het aspect informatiebeveiliging aan management, College en Raad. Adviseert over en voert maatregelen in op basis van de BIO.

Functionaris Gegevensbescherming (FG)
De FG heeft de volgende wettelijke taken (AVG Art 39), vertaald naar de situatie bij de gemeente:
- Informeren en adviseren van het College, het management, de raad en de medewerkers over hun verplichtingen met betrekking tot gegevensbescherming, tevens contactpersoon.
- Toezien op de naleving van zowel de AVG als alle andere wet- en regelgeving met betrekking tot persoonsgegevens. Hierbij hoort tevens toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

- Desgevraagd adviseren omtrent gegevensbescherming effectbeoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, en toezien op de uitvoering daarvan en het ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen;
- Toezichthouden op de registraties en afhandeling van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en toezichthouden op het melden van een datalek bij de Autoriteit en Persoonsgegevens en bij de betrokkenen.
- Samenwerken met en als contactpunt optreden voor de Autoriteit Persoonsgegevens (AP);
- Brengt verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, zijnde in veel gevallen de gemeentesecretaris, het college of de burgemeester en in sommige gevallen de gemeenteraad.

Interne controle (auditor)
De controller of auditor maar ook de FG verzorgt de interne controle op (het functioneren van) de beveiligingsorganisatie en geeft hierover gevraagd en ongevraagd advies aan de CISO. De interne controle is gemachtigd om op eigen initiatief, steekproefsgewijs, controles uit te voeren op een juiste uitvoering van het beleid door de gemeente . Dit kan bijvoorbeeld betrekking hebben op de controle op de voortgang van het uitvoeren van de maatregelen uit het informatiebeveiligingsbeleid of jaarplan. Over de resultaten van de uitgevoerde audits wordt door de lijnverantwoordelijken gerapporteerd aan de CISO. De CISO bundelt deze bijdragen en rapporteert hierover periodiek aan het college of management.