Koggenland

GEMEENTEBLAD

Officiële uitgave van de gemeente Koggenland

Nr. 486076

12 november 2025

Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Koggenland 2026 tot 2030

Managementsamenvatting

De gemeente Koggenland zet met dit strategisch informatiebeveiligingsbeleid voor de periode 2026 tot 2030 een volgende stap in het waarborgen van de betrouwbaarheid, veiligheid en continuïteit van haar informatievoorziening. Dit beleid vervangt het eerdere beleid uit 2022 en sluit aan op actuele wet- en regelgeving, zoals de Cyberbeveiligingswet (NIS2), de Algemene Verordening Gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de richtlijnen uit de Baseline Informatiebeveiliging Overheid (BIO) en NEN-ISO/IEC 27001 en 27002:2022.

Het beleid is richtinggevend en kaderstellend en wordt op tactisch en operationeel niveau verder uitgewerkt via aanvullende beleidsdocumenten, jaarplannen, maatregelen, procesbeschrijvingen en werkinstructies. Jaarlijkse actualisatie vindt plaats in lijn met de Planning & Controlcyclus, risicoanalyses, ENSIA-audits en relevante dreigingen of incidenten.

Doel en ambitie
De hoofddoelstelling is het structureel en aantoonbaar inrichten van informatiebeveiliging binnen de gehele organisatie. De gemeente streeft naar het volledig behalen van volwassenheidsniveau 4 (beheerst en meetbaar) op het gebied van informatiebeveiliging, waarbij de effectiviteit van de beheersmaatregelen periodiek wordt geëvalueerd. Dit geldt in het kader van NIS2, ISO 27001 en de BIO. En volwassenheidsniveau 3 (gedefinieerd) op het gebied van privacy. Daarbij ligt de nadruk niet alleen op compliance, maar ook op bewustwording, risicomanagement en continue verbetering.

Strategisch kader en verantwoordelijkheden
De gemeente conformeert zich aan de BIO en werkt volgens het risicomanagementproces zoals beschreven in de ISO/IEC 27001. Informatiebeveiliging wordt benaderd als een cyclisch proces: plannen, uitvoeren, controleren en bijsturen. Inwoners, ondernemers en maatschappelijke partners mogen rekenen op een betrouwbare digitale overheid.
Op basis van de Cyberbeveiligingswet (NIS2) voldoet de gemeente aan de zorg-, meld- en registratieplichten. Deze verplichtingen worden ingevuld aan de hand van tien beheersmaatregelen, waaronder risicoanalyses, incidentbeheer, weerbaarheid van toeleveranciers en fysieke beveiliging. Bestuurders en directie volgen de tien principes voor informatiebeveiliging, om eigenaarschap en bestuurlijke verantwoordelijkheid expliciet te maken.

Het beleid is tevens van toepassing op operationele technologie (PA/OT) zoals gebouwbeheersystemen en gemalen. Hiervoor wordt de Cybersecurity Implementatie Richtlijn (CSIR) toegepast.

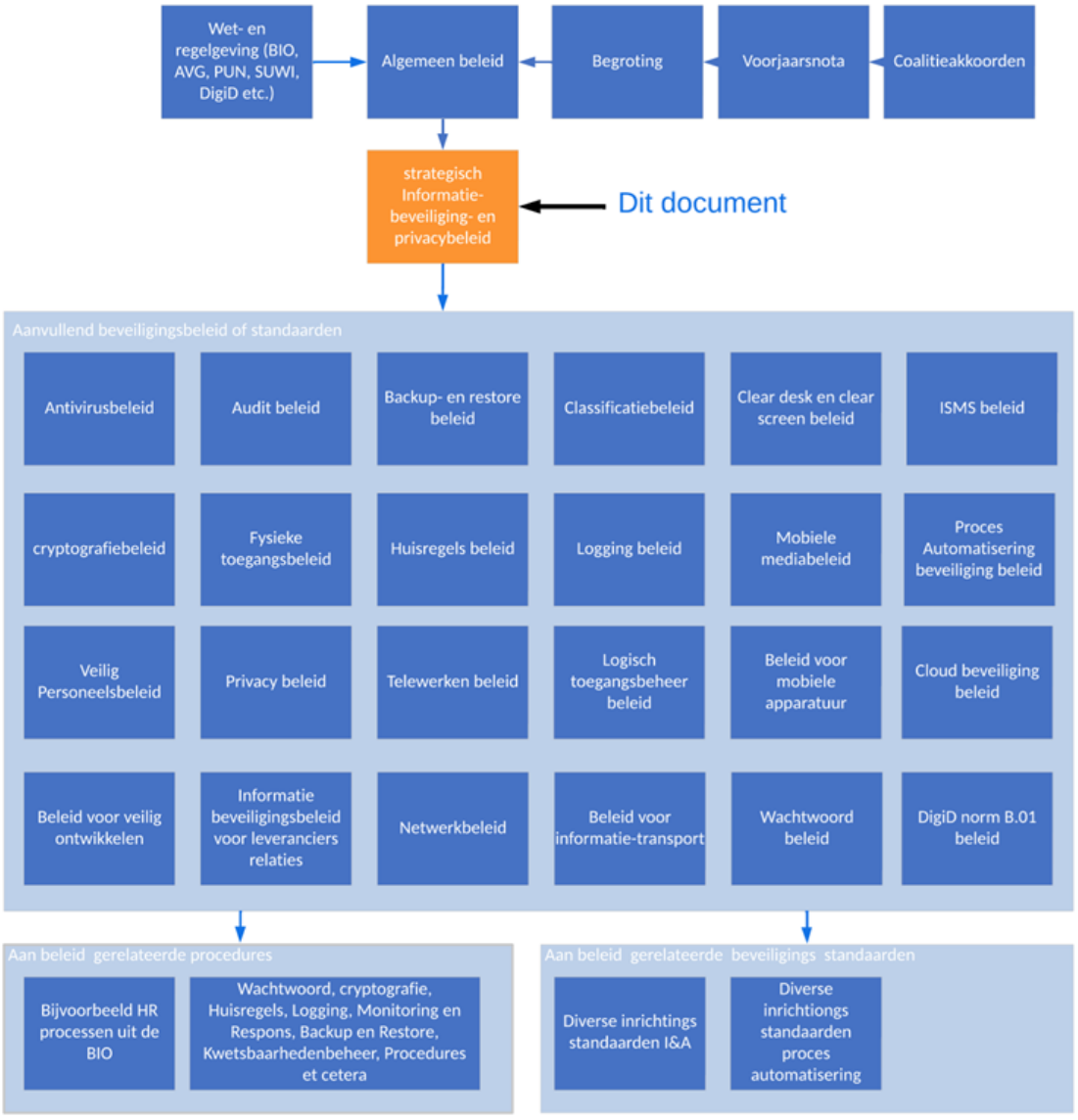
Informatiebeveiligingscultuur en kernprincipes
De gemeente investeert in een organisatiecultuur waarin informatiebeveiliging en privacy fundamentele onderdelen zijn van alle processen en diensten. Het beleid rust op de volgende vijf kernprincipes:
- Beschikbaarheid: Informatie is beschikbaar wanneer nodig, ook bij verstoringen.
- Integriteit: Informatie is juist, volledig en actueel.
- Vertrouwelijkheid: Alleen geautoriseerde personen hebben toegang tot gevoelige gegevens.
- Authenticiteit: Informatie is afkomstig van de juiste bron en niet vervalst.
- Controleerbaarheid: Toegang en gebruik van systemen zijn inzichtelijk en toetsbaar.

Privacy en gegevensbescherming
Koggenland onderkent het toenemende belang van privacy in de digitale samenleving. De omgang met persoonsgegevens is afgestemd op de AVG en gebaseerd op transparantie, zorgvuldigheid en beveiliging. Hiervoor hanteert de gemeente een separaat, aanvullend privacybeleid.

Toepassingsgebied
Het beleid is van toepassing op alle gemeentelijke processen, informatiesystemen, data en infrastructuur – en geldt voor bestuurders, medewerkers, inwoners, leveranciers en ketenpartners. Informatiebeveiliging overstijgt ICT en raakt de gehele organisatie.

Tot slot

Met dit beleid zet de gemeente Koggenland in op een veilige, wendbare en toekomstbestendige informatiehuishouding, waarin technologische ontwikkelingen, maatschappelijke verwachtingen en wettelijke verplichtingen op samenhangende wijze worden geïntegreerd. Na vaststelling door het managementteam en het college van B&W treedt dit strategisch beleid formeel in werking.



1. Inleiding

Deze beleidsnota beschrijft het Strategisch Gemeentelijk Informatiebeveiligingsbeleid voor de jaren 2026 tot 2030 en vervangt het in 2022 vastgestelde 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Koggenland 2022 tot 2026'. Het informatiebeveiligingsbeleid wordt minimaal jaarlijks en in aansluiting bij de (bestaande) bestuurs- en Planning & Control (P&C) -cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld (BIO: 5.01.02).
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau. Dit document treedt in werking na formele goedkeuring van het managementteam en college van B&W.

Met dit 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2026 tot 2030' zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit

strategisch beleid is de NEN-ISO/IEC 27002:2022 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO[1]) en het VNG Borgingsproduct AVG versie 3.0[2].

Daarnaast is bij het opstellen van dit beleid nadrukkelijk rekening gehouden met de implementatie van de Europese NIS2-richtlijn, die in Nederland is omgezet in de Cyberbeveiligingswet. Deze wet stelt aanvullende eisen aan onder andere risicobeheersing, incidentenmelding, ketenverantwoordelijkheid en toezicht, die van toepassing zijn op (vitale) gemeentelijke processen en informatiesystemen. De gemeente Koggenland valt als essentiële entiteit onder de reikwijdte van deze wet en is daarmee wettelijk verplicht te voldoen aan de daarin opgenomen zorgplicht- en de tien voorgeschreven zorgplichtmaatregelen.

De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen[3] uit de AVG voor het verwerken van persoonsgegevens.

1.1 Leeswijzer
In hoofdstuk 2 wordt de kern van het Strategisch Gemeentelijk Informatiebeveiligingsbeleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligings- en privacy plan (afdelingsplannen) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingshoofden, teamleiders, de CISO, de privacyfunctionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van de ENSIA, risicoanalyses en DPIA's. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Informatiebeveiliging
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid), vertrouwelijkheid en controleerbaarheid van (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

Kernpunten van informatiebeveiliging zijn:
- Beschikbaarheid (of continuïteit): Het zorgdragen voor het beschikbaar zijn van informatie en Informatieverwerkende systemen op het juiste moment en voor de juiste gebruikers. Gebruikers moeten kunnen vertrouwen op de continuïteit van de informatievoorziening.
- Integriteit: Het waarborgen van de correctheid, volledigheid en actualiteit van informatie. Informatie moet overeenkomen met de werkelijkheid en niet ongeautoriseerd zijn gewijzigd.
- Vertrouwelijkheid: Het beschermen van informatie tegen ongeoorloofde toegang en wijziging. Alleen geautoriseerde personen mogen toegang hebben tot gevoelige gegevens.

Daarnaast zijn er aanvullende principes die in veel organisaties eveneens belangrijk worden geacht:
- Controleerbaarheid: Het waarborgen dat toegang tot gegevens en de werking van systemen zowel tijdens gebruik als achteraf controleerbaar zijn. Dit is essentieel voor verantwoording, toezicht en forensisch onderzoek.
- Authenticiteit: De zekerheid dat informatie daadwerkelijk afkomstig is van de beweerde bron en niet is vervalst. Dit helpt om identiteitsfraude en manipulatie te voorkomen.

1.3 Privacy & Gegevensbescherming (AVG)
De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

1) https://bio-overheid.nl/
2) https://www.informatiebeveiligingsdienst.nl/avg-borgingsproduct-3-0/
3) De AVG in het kort | Autoriteit Persoonsgegevens

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat. De gemeente Koggenland heeft een separaat Privacybeleid: Privacybeleid Gemeente Koggenland | Lokale wet- en regelgeving

1.4 ISMS
De in dit beleid vastgelegde ambitie, visie, doelstellingen en uitgangspunten vormen de basis voor het Information Security Management System (ISMS) van de gemeente Koggenland. Het ISMS vertaalt deze beleidsdoelen naar concrete maatregelen, processen en controles en borgt dat informatiebeveiliging en privacy structureel worden beheerd en verbeterd. Beleid en ISMS zijn onlosmakelijk met elkaar verbonden: beleidsdoelen sturen het ISMS, terwijl uitvoering, monitoring en evaluatie binnen het ISMS leiden tot bijstelling en verfijning van beleid.

De verantwoordelijkheden rond informatiebeveiliging en privacy zijn ingericht volgens het Three Lines Model en beschreven in dit beleid (paragraaf 3.1 t/m 3.3). In het ISMS worden deze verantwoordelijkheden nader uitgewerkt en vertaald naar concrete taken, activiteiten en jaarplannen.

De uitvoering van het ISMS volgt de Plan-Do-Check-Act-cyclus: beleidsdoelstellingen worden vertaald naar risicoanalyses, maatregelen en jaarplannen (Plan), maatregelen worden uitgevoerd binnen de organisatie (Do), de werking ervan wordt getoetst door audits en controles (Check), waarna verbeteringen en beleidsaanpassingen worden doorgevoerd (Act). Documentatie en resultaten worden vastgelegd in de aangewezen systemen, waarmee de uitvoering aantoonbaar en toetsbaar is.

Door deze werkwijze vormen beleid en ISMS samen een geïntegreerd en dynamisch geheel, waarmee de gemeente Koggenland borgt dat informatiebeveiliging en privacy op alle niveaus effectief en aantoonbaar worden uitgevoerd.

1.5 Ambitie en visie van de gemeente op het gebied van informatieveiligheid en privacy
De hoofddoelstelling van dit informatiebeveiligingsbeleid is het richting geven aan het inrichten van informatiebeveiliging binnen de gemeente. Er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en middelen aangegeven waarmee dit beleid moet worden vormgegeven. Informatie is een belangrijk bedrijfsmiddel dat de gemeente Koggenland op gepaste wijze wil beschermen. Daarom is het volgende doel gesteld voor informatiebeveiliging:

De gemeente Koggenland is een betrouwbare partner voor al haar inwoners, bedrijven en ketenpartners.

De gemeente streeft ernaar om het volwassenheidsniveau van haar informatiebeveiliging op een hoog niveau te houden, met als doel volwassenheidsniveau 4: Beheerst en Meetbaar volledig te behalen. Dit geldt in het kader van NIS2, ISO 27001 en de BIO.

Het volwassenheidsniveau 4 houdt in dat de informatiebeveiliging niet alleen op strategisch niveau is geïntegreerd, maar dat alle processen goed beheerst en meetbaar zijn. Dit betekent dat de gemeente in staat is om haar informatiebeveiligingsmaatregelen effectief te monitoren, de resultaten systematisch te evalueren en deze op basis van meetbare gegevens waar nodig bij te sturen. Het beleid wordt continu gemonitord en de werking ervan is aantoonbaar en transparant.

Niveau	Naam	Omschrijving	Criteria
1	Initieel	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

Figuur 1: volwassenheidsniveau[4]

Onze ambitie is om een veilige en betrouwbare digitale omgeving te bieden, waarin zowel de persoonsgegevens van onze inwoners als andere belangrijke informatie zorgvuldig wordt behandeld. Dit wordt

4) https://www.norea.nl/nieuws/volwassenheidsmodel-voor-informatiebeveiliging-30

bereikt door robuuste beveiligingsmaatregelen te treffen die de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens waarborgen.

De gemeente Koggenland streeft ernaar een cultuur van informatiebeveiliging te creëren waarin beveiliging en privacy als fundamentele pijlers van alle gemeentelijke processen worden beschouwd. Dit beleid richt zich dan ook niet alleen op compliance, maar op een proactieve aanpak van de veiligheid en privacy van gegevens, waarin risicomanagement, bewustwording en training van medewerkers centraal staan.

Met de implementatie van de Baseline Informatiebeveiliging Overheid (BIO) en de NEN-ISO/IEC 27002:2022 standaarden wordt het beleid verder vormgegeven. Wij erkennen de dynamiek van technologische ontwikkelingen en wetgeving en zorgen ervoor dat het beleid zich blijft aanpassen aan de steeds veranderende dreigingen en eisen.

Op het gebied van privacy is de ambitie om volwassen niveau 3 (vastgesteld proces) privacybeleid te voeren, dit volgens het privacy volwassenheidsmodel[5]. De gemeente Koggenland heeft een separaat Privacybeleid: Privacybeleid Gemeente Koggenland | Lokale wet- en regelgeving

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid voor de jaren 2026 tot 2030'. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligings- en privacy plan (afdelingsplannen). Het beleid op informatiebeveiliging en privacy dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

2.2 Ontwikkelingen

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

2.2.1 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de afdelingshoofden en teamleiders nu meer dan vroeger, t.o.v. het beleid tot 2026, moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De AVG

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Koggenland is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de AVG).

2.2.3 De WPG

De gemeente heeft BOA's (Buitengewone Opsporingsambtenaren) in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (WPG). Hiervoor moet de gemeentebeleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht

2.2.4 De NIS2-richtlijn/ Cyberbeveiligingswet

De gemeente Koggenland erkent het belang van de NIS2-richtlijn en de Cyberbeveiligingswet in het kader van de versterking van de cyberbeveiliging binnen de Europese Unie en Nederland. Deze wetgeving legt een aantal cruciale verplichtingen op aan organisaties die als essentieel worden aangemerkt, en beoogt de digitale weerbaarheid te verhogen door het afdwingen van zorgvuldige beveiligingsmaatregelen en een adequaat meldproces.

Zorgplicht

De Cyberbeveiligingswet verplicht de gemeente tot het nemen van passende maatregelen ter bescherming van haar netwerk- en informatiesystemen tegen significante incidenten, zoals cyberaanvallen en andere verstoringen die schade kunnen veroorzaken. De wet stelt tien zorgplichtmaatregelen vast, waaronder het uitvoeren van risicoanalyses, het implementeren van beveiligingsmaatregelen op het

5) https://www.cip-overheid.nl/media/uasdokan/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

gebied van personeel en toegangsbeheer, en het waarborgen van de bedrijfscontinuïteit. Het bestuur van de gemeente is verantwoordelijk voor het goedkeuren van deze maatregelen en dient toezicht te houden op de uitvoering ervan.

Registratieplicht
Volgens de Cyberbeveiligingswet is de gemeente verplicht om zich te registreren bij het Nationaal Cyber Security Centrum (NCSC), waarmee zij haar naleving van de wet bevestigt. De registratie draagt bij aan de transparantie en versterking van de digitale weerbaarheid binnen de EU. Organisaties moeten zich via het NCSC-portaal registreren, hetgeen een verplichting wordt na de inwerkingtreding van de wet.

Meldplicht
De gemeente is verplicht om significante cyberincidenten, die de dienstverlening ernstig verstoren of aanzienlijke schade veroorzaken, binnen 24 uur na ontdekking te melden. Na de eerste melding volgt een vervolgmelding binnen 72 uur, en een eindverslag moet uiterlijk één maand na het incident worden ingediend. Deze meldingen worden gedeeld met het sectorale Computer Security Incident Response Team (CSIRT) en de toezichthouder. Het doel van deze meldplicht is om snel te kunnen reageren op incidenten en zo nodig bijstand te verlenen, waardoor de impact op de dienstverlening wordt geminimaliseerd.

2.2.5 De 10 principes voor informatiebeveiliging[6]
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader 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. Als 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.

2.2.6 De 10 zorgplichtmaatregelen[7]
De gemeente Koggenland valt onder de reikwijdte van de Cyberbeveiligingswet en is daarmee verplicht om te voldoen aan de daarin opgenomen zorgplicht. Deze zorgplicht houdt in dat passende en evenredige beveiligingsmaatregelen genomen moeten worden om netwerk- en informatiesystemen te beschermen tegen significante incidenten.

De gemeente hanteert daarbij de tien voorgeschreven zorgplichtmaatregelen, die gericht zijn op het verhogen van de digitale weerbaarheid en het waarborgen van de continuïteit van essentiële diensten:
- Uitvoeren van risicoanalyses en beveiliging van informatiesystemen
- Beveiliging van personeel, toegangsbeheer en beheer van bedrijfsmiddelen
- Voorzien in bedrijfscontinuïteit, zoals back-ups en noodplannen
- Inrichting van incidentenbeheer
- Bevordering van basis cyberhygiëne en trainingen voor medewerkers
- Beveiliging bij ontwikkeling en onderhoud van systemen
- Beveiliging van de toeleverancierskeketen
- Beleid en procedures voor cryptografie en encryptie
- Gebruik van multifactorauthenticatie en beveiligde communicatie
- Evaluatie en continue verbetering van beheersmaatregelen

6) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
7) https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn

Het college van burgemeester en wethouders is verantwoordelijk voor het goedkeuren en toezicht houden op de uitvoering van deze maatregelen, en volgt hiervoor de benodigde opleidingen, zoals voorgeschreven in de wet.

2.2.7 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

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

2.2.8 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem biedt waardevolle inzichten en vormt een belangrijke bron van leerervaringen. Incidenten uit het verleden worden dan ook nadrukkelijk betrokken bij het actualiseren van het informatiebeveiligingsbeleid. De gemeente hanteert hiervoor een vastgesteld beleid voor Incidentmanagement en Response (IM&R), waarin verantwoordelijkheden, opvolging en afhandeling van incidenten zijn geregeld. Ook het datalekkenproces is hierin opgenomen, inclusief de werkwijze voor signalering, beoordeling, melding en documentatie van datalekken, conform de AVG.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2022. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2022 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[8] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.
De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacy plan (afdelingsplannen) zal deze structuur volgen.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsafdelingen die zich met PA bezighouden.[9] Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR). [10]

2.4 Plaats van het strategisch beleid

Het Strategisch Gemeentelijk Informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau.

Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Dit beleid zal worden vertaald in aanvullend beleid en tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven ‘Gemeentelijk Informatiebeveiligings- en privacy plan’ (afdelingsplannen).

2.5 Scope informatiebeveiliging en privacy

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

Dit Strategisch Gemeentelijk Informatiebeveiligingsbeleid vormt een algemene basis en dekt tevens aanvullende beveiligingseisen uit relevante wet- en regelgeving, zoals de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden, op basis van deze regelgeving, aanvullende specifieke beveiligingseisen (zoals voor SUWI, gemeentelijke basisregistraties en DigiD met norm B.01). Deze eisen worden uitgewerkt in aanvullende beleidsdocumenten.

8) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*
9) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
10) https://www.cert-wm.nl/csir

Het beleid is opgesteld met inachtneming van de toekomstvisie, missie en kernwaarden van de gemeente Koggenland en het coalitieprogramma.

Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

Alle informatie en informatiesystemen zijn van belang voor de gemeente, waarbij bepaalde informatie van vitaal of kritiek belang is. Het college van B&W is eindverantwoordelijk voor informatiebeveiliging en privacy, voor alle gemeentelijke informatiesystemen, ongeacht waar deze worden gehost.

Dit beleid geldt tevens voor alle Procesautomatiseringssystemen (PA) die eigendom zijn van de gemeente en die worden gebruikt binnen gemeentelijke gebouwen of in de publieke ruimte. Denk hierbij aan gebouwbeheersingssystemen, pompen en gemalen. Ook deze systemen vallen onder de reikwijdte van dit strategisch informatiebeveiligingsbeleid.

2.6 Uitgangspunten
Het bestuur, het managementteam en de teamleiders spelen een cruciale rol bij het uitvoeren van dit Strategisch Gemeentelijk Informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de (privacy) risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging en privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en privacy en demonstreert dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een Strategisch Gemeentelijk Informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Het beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Business Continuity Management
De gemeente hanteert een Business Continuity Management (BCM)-beleid dat ervoor zorgt dat essentiële processen kunnen worden voortgezet bij verstoringen, zoals cyberincidenten, stroomuitval of andere calamiteiten. Onder BCM-maatregelen vallen onder andere back-upstrategieën, rampenherstelplannen (disaster recovery) en het periodiek testen en actualiseren van continuïteitsplannen om de paraatheid te waarborgen.

2.6.2 Strategische doelen
De strategische doelen van het Strategisch Gemeentelijk Informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.6.3 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Koggenland hebben een interne eigenaar die de vertrouwelijkheid, privacy eisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.

- Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het beleid vormt samen met het IB&P plan (afdelingsplannen) het fundament onder een betrouwbare informatievoorziening en privacybescherming. In het IB&P plan (afdelingsplannen) wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy.
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Het borgen van privacy in de uitvoering van gemeentelijke processen vindt risico gestuurd plaats. De verantwoordelijken in de organisatie maken afwegingen ter naleving van privacyregels en op basis van een risico-inschatting.

2.6.4 IB&P governance

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college van B&W stelt als eindverantwoordelijke het Strategisch Gemeentelijk Informatiebeveiligingsbeleid vast.
- Het directie- managementteam stelt jaarlijks het IB&P plan (afdelingsplannen) vast.
- Het managementteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- Het managementteam is verantwoordelijk voor het vragen om informatie bij de teamleiders en ziet erop toe dat de teamleiders adequate maatregelen nemen voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid vallen.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het directie- managementteam, voorafgaand aan de P&C-cyclus.
- De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
- Het managementteam en de teamleiders stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de functionaris gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- Tijdens Planning & Control-cyclus dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teamleiders zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- Het breed (groot) managementteam is verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals DigiD, BRP/ reisdocumenten, BAG/ BGT/ BRO en Suwinet) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.

- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.
- Teamleiders dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teamleiders voeren met behulp van de CISO, PO of FG, QuickScans informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's uit op basis van de AVG uit om deze risico-afwegingen te kunnen maken.
- Informatiebeveiliging en privacybescherming maakt deel uit van de beoordelingssystematiek en wordt besproken tussen de teamleider en de medewerker.

2.6.5 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB&P plan (afdelingsplannen) opgesteld onder leiding van de CISO, gebaseerd op:
- Dit Strategisch Gemeentelijk Informatiebeveiligingsbeleid;
- De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
- Andere audit resultaten;
- Het dreigingsbeeld gemeenten van de IBD;
- Uitkomsten risicoanalyses en DPIA's;
- De door de teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).
- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P plan (afdelingsplannen) worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

2.6.6 Ketensamenwerking

De gemeente Koggenland werkt intensief samen met ketenpartners en leveranciers bij de uitvoering van haar taken. Informatiebeveiliging is een vast onderdeel van deze samenwerking en wordt expliciet opgenomen in contracten, dienstverleningsovereenkomsten en aanbestedingen. Daarbij hanteert de gemeente een Programma van Eisen (PvE) Informatiebeveiliging, dat is gebaseerd op de normen ISO/IEC 27001 en 27002, evenals de uitgangspunten van de Baseline Informatiebeveiliging Overheid (BIO).

De gemeente beoordeelt of ketenpartners voldoen aan deze eisen, zowel bij de inkoop als tijdens de samenwerking. Periodiek wordt geëvalueerd of de afgesproken beveiligingsmaatregelen nog toereikend zijn en worden waar nodig aanvullende afspraken gemaakt.

2.6.7 Beveiligingsbewustzijn

Informatiebeveiliging is geen statisch document dat alleen op papier bestaat; het is een dynamisch proces dat door de hele organisatie moet worden gedragen. Het doel van het informatiebeveiligingsbeleid van de gemeente Koggenland is om een stevige basis te leggen voor een veilige en verantwoorde omgang met informatie binnen de organisatie. Het beleid is daarom niet alleen bedoeld voor een selecte groep, maar raakt alle medewerkers, beheerders en bestuurders op verschillende manieren.

De gemeente onderscheidt drie doelgroepen:

1. **Medewerkers die werken met informatiesystemen**
   Het is van cruciaal belang dat alle medewerkers de basisprincipes van informatiebeveiliging kennen en toepassen in hun dagelijks werk. De gemeente zorgt voor periodieke bewustwordingscampagnes om medewerkers structureel te informeren over deze principes. Dit gebeurt via verschillende kanalen, zoals intranetberichten, workshops en e-learning modules. Daarnaast voert de gemeente periodiek social engineering-tests uit, zoals phishingcampagnes, om de bewustwording te verhogen en het gedrag van medewerkers te verbeteren. Bij indiensttreding krijgen nieuwe medewerkers de mogelijkheid om zich in te schrijven voor het Privacy, Informatiebeveiliging en AVG Introductieprogramma, waarin ze worden voorbereid op de basiseisen rondom informatiebeveiliging.
2. **Beheerders van informatiesystemen**

Voor de applicatiebeheerders binnen de gemeente geldt een verhoogde verantwoordelijkheid. Specifieke aandachtspunten voor deze groep zijn onder andere de bijzondere positie van beheerdersaccounts, dataclassificatie, en de bescherming van gevoelige gegevens, zoals persoonsgegevens. Daarnaast moeten beheerders zich bewust zijn van de procedures voor incidentbeheer, back-up en restore en bedrijfscontinuïteit. Regelmatige training en het volgen van richtlijnen en procedures op het gebied van IT-beveiliging is cruciaal om risico's te minimaliseren.

3. **Bestuurders, managementteam en afdelingsmanagement**
   Voor het bestuur, managementteam en afdelingshoofden zijn de volgende onderwerpen van belang: de beveiligingsverantwoordelijkheden binnen hun afdelingen, personeelsprocessen (in- en uitdiensttreding), risicomanagement en de koppeling tussen beveiliging en inkoop. Leidinggevenden dienen goed op de hoogte te zijn van de beveiligingsmaatregelen en de impact die deze hebben op de organisatie. Ook hun verantwoordelijkheid ten aanzien van privacy en dataclassificatie is essentieel. Om deze verantwoordelijkheid te kunnen dragen, dienen bestuurders en afdelingsmanagers periodiek te worden getraind en begeleid in het beheren van de risico's die voortkomen uit de digitale werkomgeving.

Naast het gebruik van de juiste middelen is het essentieel dat alle medewerkers zich bewust zijn van de risico's die de digitale wereld met zich meebrengt. Dit bewustzijn wordt ondersteund door trainingen en bewustwordingsprogramma's. Medewerkers worden geïnformeerd over zowel de kansen als de risico's van digitaal werken, met speciale aandacht voor de bescherming van vertrouwelijke gegevens. Het training- en bewustwordingsprogramma wordt jaarlijks bijgewerkt en omvat onderwerpen zoals cybercrime, phishing, social engineering, en veilig werken op afstand.
De effectiviteit van informatiebeveiliging hangt voor een groot deel af van de kennis, bewustwording, en het gedrag van de medewerkers. Het is de verantwoordelijkheid van iedere medewerker om de aangeboden kennis op te nemen en toe te passen. Leidinggevenden spelen hierin een cruciale rol door het bevorderen van een professionele houding en het ondersteunen van medewerkers bij het naleven van de informatiebeveiligingsmaatregelen.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense'). In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO, PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA-coördinator.

3.1 Aansturing: managementteam

Het managementteam zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De afdelingshoofden zorgt dat de teamleiders zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het managementteam zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het managementteam stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het managementteam draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacy beleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO of FG van de gemeente. Het managementteam autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de gemeente Koggenland gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: teamleiders

Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle teamleiders. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, (persoons)gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teamleiders rapporteren aan de afdelingshoofden over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het breed (groot) managementteam overleg.

Taken van de afdelingsmanagers in het kader van informatiebeveiliging (die ondersteund worden door de CISO) en privacybescherming zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht zijn.
- Het binnen de eigen afdeling uitdragen van het Strategisch Gemeentelijk Informatiebeveiligingsbeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld. Het vroegtijdig betrekken van CISO en PO (of FG) bij nieuwe of gewijzigde processen.
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die deze moeten hebben voor beleid en maatregelen.

3.3 Controle en verantwoording

Dit Strategisch Gemeentelijk Informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de gemeente Koggenland. De bestuurders, management en teamleiders van de gemeente Koggenland zullen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.

Het managementteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. Het managementteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. Deze rapportages zijn afkomstig CISO en FG.

3.3.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dit betekent dat er een ENSIA-coördinator is aangewezen die ervoor zorgt dat de benodigde informatie bij de verantwoordelijke vakspecialisten en teamleiders wordt opgehaald. Deze vakspecialisten en teamleiders leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging en privacybescherming komt tot uitdrukking in het jaarverslag, via de collegeverklaring Informatiebeveiliging en Privacy. In deze verklaring geeft het college van B&W aan in hoeverre de gemeente voldoet aan de afspraken die zijn gemaakt voor de ENSIA-verantwoording, evenals aan de wettelijke eisen zoals de AVG. Ook worden eventuele verbetermaatregelen vermeld die de gemeente zal treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de gemeenteraad.

Via ENSIA verantwoordt de gemeente zich zowel horizontaal aan de gemeenteraad (interne toezichthouder) als verticaal aan de centrale toezichthouders[11] van de informatiestelsels, zoals DigiD, BRP/reisdocumenten, BAG/BGT/BRO en Suwinet.

Evaluaties uit de ENSIA-verantwoording en risicoanalyses leiden tot verbetermaatregelen die worden opgenomen in het Gemeentelijk Informatiebeveiligings- en Privacyplan. De voortgang van deze maatregelen wordt bewaakt door het managementteam en de CISO, en wordt jaarlijks gerapporteerd aan het college van B&W.

Met deze verantwoording wordt het bestuur van de gemeente Koggenland en de gemeenteraad geïnformeerd. De betrokkenheid van het bestuur is essentieel en toont aan dat de gemeente Koggenland informatiebeveiliging en privacybescherming serieus neemt. En het laat zien dat het een integraal onderdeel is van de ambities om de informatie van haar inwoners adequaat te beschermen.

11) https://vng.nl/projecten/ensia