Gemeente Landsmeer

GEMEENTEBLAD

Officiële uitgave van de gemeente Landsmeer

Nr. 424946

1 oktober

2025

Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente Landsmeer

besluit:

Het bijgaande Strategisch Informatiebeveiligingsbeleid Landsmeer 2025 vast te stellen onder gelijktijdige intrekking van het bestaande beleid uit 2024;

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid en vervangt het in 2024 vastgestelde 'strategisch informatiebeveiligingsbeleid'. Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit strategisch beleid zet de gemeente een volgende stap in het borgen van de beveiliging van persoonsgegevens en andere informatie, en bouwt zij voort op de maatregelen en ontwikkelingen van de afgelopen jaren. De basis hiervoor wordt gevormd door de NEN-ISO/IEC 27002:2022 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Daarnaast zijn bij de totstandkoming van dit beleid de 10 principes voor informatiebeveiliging van de VNG als uitgangspunt gehanteerd.

Dit beleid houdt tevens rekening met actuele en aankomende wet- en regelgeving op het gebied van cybersecurity, waaronder de Europese NIS2-richtlijn en de nationale Cyberbeveiligingswet (CBW). Hiermee wordt geborgd dat de gemeente niet alleen voldoet aan bestaande normen en verplichtingen, maar ook tijdig inspeelt op veranderende eisen en dreigingen in het digitale domein.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid 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 actieplan informatiebeveiliging (vastgesteld door het managementteam) worden deze tactische en operationele aspecten van informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de teammanagers, de CISO, het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist.

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) en vertrouwelijkheid van (persoons)gegevens en andere informatie.

Onder informatiebeveiliging van de gemeente Landsmeer verstaan we de passende bescherming van beschikbaarheid, integriteit en vertrouwelijkheid ("BIV") van informatie die door of onder verantwoordelijkheid van de gemeente Landsmeer wordt verwerkt:

- **Vertrouwelijkheid**: Dit gaat over de gevoeligheid van gegevens en de schade wanneer deze "op straat" komen te liggen of in handen van onbevoegden. Een hoge vertrouwelijkheid is bijvoorbeeld nodig voor gezondheidsgegevens in Wmo- en Jeugdwetaanvragen.
- **Integriteit**: Dit gaat over de juistheid, actualiteit en authenticiteit van gegevens en de schade wanneer gegevens onbevoegd worden gewijzigd. Een hoge integriteit is bijvoorbeeld nodig bij betalingsgegevens met een frauderisico.
- **Beschikbaarheid**: Dit gaat over de beschikbaarheid van informatie voor de bedrijfsprocessen en de schade die ontstaat wanneer een bedrijfsproces tijdelijk niet uitgevoerd kan worden. Een hoge beschikbaarheid is bijvoorbeeld nodig bij de basisregistraties.

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 de raad, het bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie en visie van de gemeente

De ambitie van de gemeente is efficiënt en effectief gebruik te maken van mensen en middelen ten behoeve van het implementeren van passende maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen en zo het niveau van informatieveiligheid te verhogen en vast te houden. De visie van de gemeente Landsmeer is om door te groeien naar een volwassen, hechte en professionele organisatie. De ambitie ten aanzien van informatiebeveiliging sluit hier op aan. Het is van groot belang te beseffen dat 100% veiligheid niet bestaat. Er is altijd sprake van nieuwe ontwikkelingen waardoor nieuwe kwetsbaarheden en aanvalsmethoden kunnen ontstaan. Daarnaast speelt de menselijke factor een rol. Mensen kunnen beveiligingsmaatregelen omzeilen of door kwaadwillende worden verleid om een aanval te faciliteren, bijvoorbeeld door te goeder trouw op een link in een email te klikken. Het is dus onmogelijk om de risico's op het gebied van informatiebeveiliging tot nul terug te brengen. Op basis van een risicoafweging worden maatregelen genomen om inbreuken te voorkomen, te detecteren om de gevolgen van een inbreuk te beperken. Bij die risicoafweging worden de kosten van een maatregel afgewogen tegen de risicoreductie door de maatregel.

2. Strategisch beleid

2.1 Doel

Dit Informatiebeveiligingsbeleid geeft richting aan de manier waarop binnen de gemeente Landsmeer wordt gezorgd voor een adequate informatiebeveiliging en de borging daarvan. Dit beleid bevat de uitgangspunten, beschrijft de organisatie en geeft de aanpak ten aanzien van informatiebeveiliging weer. De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan. Het informatiebeveiligingsbeleid is richtinggevend en kaderstellend voor het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid 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 teammanagers nu meer dan vroeger 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 AVG stelt onder andere eisen aan Informatiebeveiliging. Daaraan wordt invulling gegeven middels het voorliggende beleid.

2.2.3 De WPG

De gemeente heeft Buitengewoon opsporingsambtenaren (Boa's) in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (Wpg). Om aan de wet politiegegevens te voldoen is het nodig dat de gemeente beleid en samenhangende procedures heeft ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht. Daaraan wordt gedeeltelijk invulling gegeven middels het voorliggende beleid.

2.2.4 NIS2

De Network and Information Security Directive 2 (NIS2) is op 17 oktober 2024 van kracht geworden binnen de Europese Unie. In Nederland wordt deze Europese richtlijn omgezet in de Cyberbeveiligingswet (Cbw). Hoewel de wet inmiddels is aangenomen en daarmee in werking is getreden, is deze nog niet van kracht. De daadwerkelijke toepassing van de Cbw wordt naar verwachting in het derde kwartaal van 2025 van kracht.

De Cbw legt aanvullende verplichtingen op aan essentiële en belangrijke entiteiten, waaronder ook gemeenten die verantwoordelijk zijn voor onderdelen van de afvalwaterketen, zoals het gemeentelijke rioolbeheer. Om zich goed voor te bereiden op de eisen van de Cbw en de onderliggende NIS2-richtlijn, werkt de gemeente Landsmeer actief aan de versterking van haar digitale weerbaarheid.
Een belangrijke stap hierin is de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Met de BIO als normenkader zorgt de gemeente voor een structurele aanpak van informatiebeveiliging en legt zij een stevige basis voor naleving van de aankomende wettelijke verplichtingen.

2.2.5 Kunstmatige intelligentie

Sinds 2022 is de ontwikkeling en toepassing van kunstmatige intelligentie (AI) in een stroomversnelling geraakt. Deze snelle opmars biedt kansen voor innovatie en efficiëntie, maar brengt ook serieuze risico's met zich mee op het gebied van informatiebeveiliging en privacy.
Zo kunnen generatieve AI-toepassingen, zoals ChatGPT, Bing Chat of andere op AI gebaseerde zoek- en communicatietools, onbedoeld leiden tot het lekken van gevoelige informatie, bijvoorbeeld wanneer vertrouwelijke gegevens via prompts worden gedeeld en mogelijk worden verwerkt of opgeslagen door externe aanbieders. Daarnaast maken kwaadwillenden actief gebruik van AI om overtuigende phishingmails te genereren, deepfakes te creëren of wachtwoorden te kraken via geavanceerde algoritmes.
De gemeente Landsmeer is zich bewust van zowel de risico's als de kansen van AI en wil zich daarom zorgvuldig oriënteren op het veilig, verantwoord, effectief en efficiënt gebruik van kunstmatige intelligentie binnen de gemeentelijke organisatie. Medewerkers moeten de ruimte krijgen om AI op een zinvolle manier in te zetten ter ondersteuning van hun werkzaamheden, mits dit gebeurt binnen duidelijke kaders voor informatieveiligheid, privacy en ethiek.

2.2.6 De 10 principes voor informatiebeveiliging[1]

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.

2.2.7 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

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

2.2.8 Cybersecuritybeeld Nederland

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) publiceert jaarlijks het Cybersecuritybeeld Nederland met daarin een analyse van de ontwikkelingen ten aanzien van cyberdreigingen.

2.2.9 Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Standaarden informatiebeveiliging

De basis en het normenkader voor de inrichting van het beveiligingsbeleid is de Baseline Informatiebeveiliging Nederlandse Overheid (BIO). Maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2022 genomen.

1) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. De BIO bestaat uit een baseline met verschillende niveaus van beveiliging.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet, bijvoorbeeld bruggen en rioolgemalen. 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 beleidsteams die zich met PA bezig houden.[3] Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR).[4]

2.4 Plaats van het strategisch beleid
Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. De gemeente voorziet ten minste de volgende tactische beleidsplannen, waarin telkens wordt beschreven hoe een deel van de beveiligings-/beheersmaatregelen binnen de gemeente worden toegepast:
- Logisch toegangsbeleid
- Fysiek toegangsbeleid
- Telewerkbeleid
- Personeel (procedure antecedentenonderzoek, indiensttreding, overplaatsing medewerker en vertrek medewerker)
- Gedragsregels informatieveiligheid voor medewerkers
- Gebruik digitale middelen
- Beveiligingsbeleid ICT
- Cryptografiebeleid
- Bedrijfscontinuïteitsplan
- Beveiligingsbeleid externe partijen (incl. leveranciers)
- BRP beveiligingsplan

2.5 Scope informatiebeveiliging
De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen in opdracht van de gemeente, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur, inclusief de griffie. Het informatiebeveiligingsbeleid en de beveiligingsmaatregelen zijn van toepassing voor de leden van de gemeenteraad voor zover zij gebruik maken van middelen, applicaties en diensten die hen door de gemeente ter beschikking zijn gesteld. Te denken valt aan tablets, telefoon, de applicatie voor raadsstukken en toegangspassen.

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI (deze afkortingen zijn uitgewerkt in bijlage 1). Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in bijlage 1 geformuleerd.

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.
Samengevat bestaat de scope uit:
- Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijk voor de informatiebeveiliging. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.
- Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.

2.6 Uitgangspunten
Voor informatiebeveiliging gaat het College van B en W van de gemeente Landsmeer uit van de volgende uitgangspunten.

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

2.6.1 Naleving

Het uitgangspunt is dat het College van B en W van de gemeente Landsmeer, het management, de Chief Information Security Officer (CISO) en de proceseigenaren (teammanagers) de naleving bevorderen van dit informatiebeveiligingsbeleid. Daarnaast bevorderen/ stimuleren zij de algehele communicatie en bewustwording (awareness) rondom informatieveiligheid.

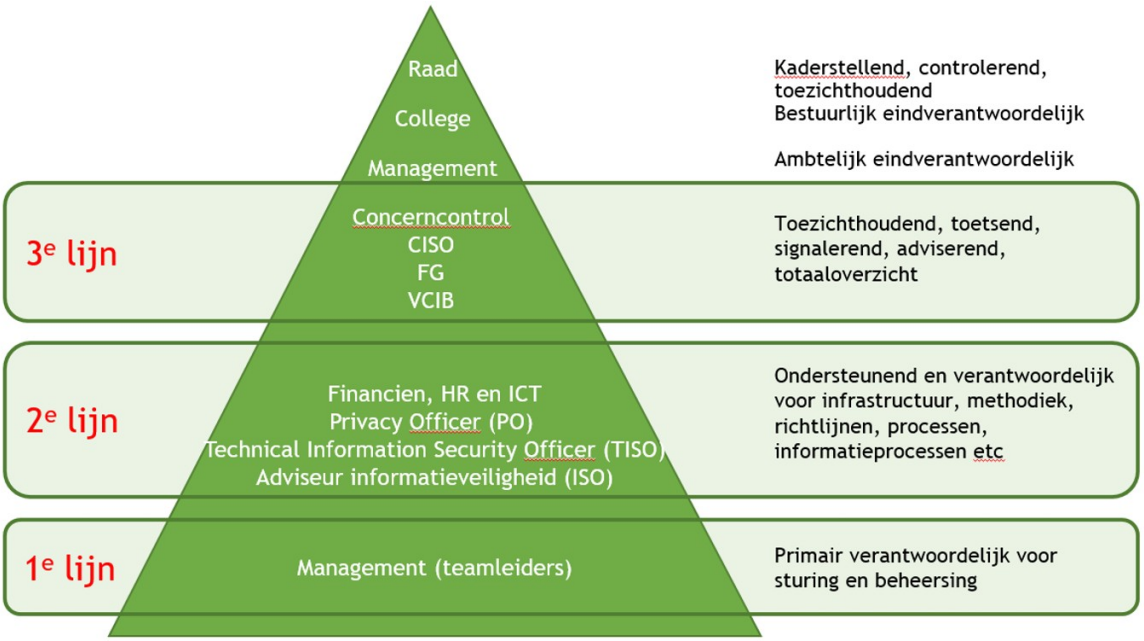
2.6.2 Drie verdedigingslinies / Three lines of defense

Het uitgangspunt is de toepassing van de Three lines of defense. Bij de toepassing van informatiebeveiliging staat het faciliteren van de werkprocessen van de organisatie voorop. Informatiebeveiliging dient hieraan een bijdrage te leveren door het veilig werken met informatie te faciliteren. Dat betekent dat maatregelen in balans zijn met de te beschermen waarde of het belang. Er moeten 'doelmatige, zakelijke' argumenten zijn om beveiligingsmaatregelen te treffen. Deze balans wordt gevonden op basis van een expliciete risicoafweging, d.w.z. de te nemen maatregelen voor informatieveiligheid zijn risico gedreven.

De organisatie wil aantoonbaar voldoen aan wet- en regelgeving. Het gaat daarbij met name om de Algemene verordening gegevensbescherming (AVG), de Wet Politiegegevens (Wpg), wetten met betrekking tot basisregistraties, zoals de Basisregistratie Personen (BRP), de Archiefwet, maar ook om wetgeving met betrekking tot specifieke taken van de gemeente zoals de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet. De AVG vereist in dit kader passende organisatorische en technische beveiligingsmaatregelen rekening houdend met de stand van de techniek, de kosten alsook de aard, omvang, context en de waarschijnlijkheid en ernst van risico's (zie Art 32 lid 1 AVG) en ook aantoonbaarheid, evaluatie en aanpassing van de maatregelen en andere verplichtingen van de AVG (Art 5 lid 2; Art 24 lid 1).

De organisatie wil "in control" zijn, dat wil zeggen overzicht hebben en risico's bewust nemen vanuit bestuurlijk niveau. Dit betekent dat eventuele (rest-)risico's die niet afgedekt (kunnen) worden door beheersmaatregelen, bijvoorbeeld omdat zij niet proportioneel worden geacht, ter acceptatie worden voorgelegd aan het management. De organisatie past daarvoor de drie verdedigingslijnen toe vanuit Interne Controle::

1. De beheersing van werkprocessen binnen de team onder verantwoordelijkheid van de teammanagers. Dat wil zeggen: werkprocessen op orde, passende werkinstructies en werken volgens afspraken. Dat betekent dat de teamen zelf 'in control' (lees, beheersing van taken) dienen te zijn door het treffen van de aan hen toegewezen adequate beheersmaatregelen en de monitoring van de werking.
2. Ondersteuning door de CISO en andere ondersteunende teamen met advies en hulpmiddelen voor beheersmaatregelen in de 1e lijn. Dit omvat ook hulpmiddelen voor en regie op borging/controle van beheersmaatregelen in de lijn, bijvoorbeeld door kwaliteitsfunctionarissen of teammanagers. Deze borgingsmaatregelen/controles hebben als doel vast te stellen en aan te tonen dat werkprocessen conform de afspraken verlopen en deze te evalueren en waar nodig aan te passen. Deze borging wordt voor informatiebeveiliging gecoördineerd door de CISO en uitgevoerd in de lijn op basis van een controleplan
3. De concerncontroller, de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) hebben een toetsende, signalerend, initiërende en adviserende rol m.b.t. de kwaliteit, de getrouwheid, rechtmatigheid en het functioneren van de 1e en 2e lijn. Onderdeel van de 3e lijn zijn interne en externe audits vanuit de stafteam Concerncontrol, onder andere de Verbijzonderde Interne Controles (VIC) en onderzoeken/audits op basis van art. 213a van de Gemeentewet, art. 33 van de Wet Politiegegevens en de diverse audits vanuit ENSIA (Eenduidige Normatiek Single Information Audit). De 3e lijn resulteert in de evaluatie van de opzet, bestaan en werking van de 1e en de 2e verdedigingslinie als basis voor de evaluatie/beoordeling door het management, college en raad.



2.6.3 Risicomanagement

Risicomanagement is een kernonderdeel van informatiebeveiliging binnen de gemeente Landsmeer en vormt de basis voor de BIO, NIS2 en de aankomende Cyberbeveiligingswet. Het uitgangspunt is dat beveiligingsmaatregelen proportioneel en risicogebaseerd worden toegepast. De aanpak bestaat uit het identificeren, analyseren en beoordelen van risico's, gevolgd door het nemen van passende maatregelen om deze te vermijden, te mitigeren, over te dragen of – na expliciete besluitvorming – te accepteren. Proceseigenaren en teammanagers voeren risicoanalyses uit voor hun processen; de CISO coördineert en bewaakt de uitvoering. Restrisico's die van strategisch belang zijn worden ter besluitvorming voorgelegd aan het college van B&W. Risicomanagement is structureel onderdeel van de jaarlijkse PDCA-cyclus, het actieplan informatiebeveiliging en de besluitvorming bij nieuwe processen en samenwerkingen. Hiermee voldoet de gemeente aantoonbaar aan de eisen van de BIO en NIS2 en borgt zij de bescherming van informatie in al haar processen en ketens.

2.6.4 Management systeem voor informatiebeveiliging (ISMS)

De gemeente Landsmeer richt een Informatiebeveiligingsmanagementsysteem (ISMS) in als gestructureerde en systematische aanpak om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te borgen. Het ISMS is gebaseerd op de ISO 27001-norm, aangevuld met de verplichte overheidsmaatregelen uit de Baseline Informatiebeveiliging Overheid versie 2 (BIO2), en voldoet aan de NIS2-richtlijn en de aankomende Cyberbeveiligingswet.

Scope

Het ISMS richt zich in eerste instantie op de kritieke processen van de gemeente Landsmeer. Deze zijn vastgesteld op basis van de gemeentelijke dataclassificatie en een Business Impact Analyse (BIA), waarbij processen zijn geselecteerd waarvan aantasting van de BIV-eigenschappen zou leiden tot onacceptabele gevolgen voor inwoners, bedrijven of samenwerkingspartners. In latere fases kan de scope worden uitgebreid naar overige processen, systemen en locaties op basis van nieuwe risicoanalyses.

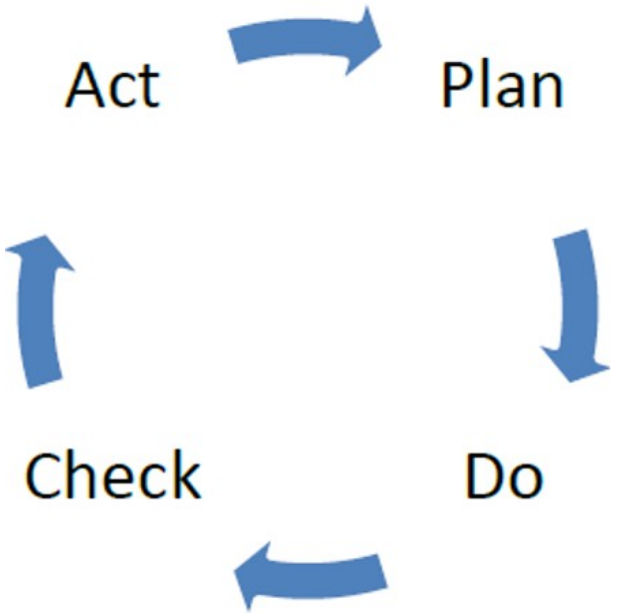
Risico gebaseerde aanpak

Het ISMS hanteert een risico gebaseerde aanpak: maatregelen worden geselecteerd en geïmplementeerd op basis van een gedegen risicobeoordeling. Hierbij wordt rekening gehouden met wettelijke verplichtingen, organisatorische context, actuele dreigingen en beschikbare middelen. Afwijkingen van de BIO2 worden uitsluitend toegepast via het "comply-or-explain"-principe en met bestuurlijke goedkeuring. Waar mogelijk maakt de gemeente gebruik van open standaarden en landelijke voorzieningen, en werkt zij samen met de Informatiebeveiligingsdienst (IBD) om uniformiteit en effectiviteit te waarborgen.

PDCA-cyclus

Het uitgangspunt is dat de gemeente Landsmeer de plan-do-check-act cyclus doorloopt voor de verbetering en beheersing van informatiebeveiliging. Het doorlopen van deze cyclus vormt het management systeem voor informatiebeveiliging (ISMS). De plan-do-check-act cyclus wordt op het niveau van de gemeente Landsmeer en op het niveau van de beheersmaatregelen toegepast:

- *Plan:* inrichten en documenteren van de beheersmaatregelen en de organisatiebrede aanpak van informatiebeveiliging op basis van geldende normen, wettelijke eisen en risico's voor de organisatie (in termen van interne controle: de opzet, 1e verdedigingslinie)
- *Do:* aantonen van de uitvoering van beheersmaatregelen en de organisatie-brede aanpak van informatiebeveiliging (in termen van interne controle: het bestaan, 1e verdedigingslinie)
- *Check:* de borging/controle en evaluatie van de beheersmaatregelen en de organisatiebrede aanpak van informatiebeveiliging met als criteria de volledige uitvoering van de maatregelen en de effectiviteit hiervan. Daarbij wordt ook rekening gehouden met de voortschrijdende ontwikkeling van de techniek en bedreigingen. Hieronder vallen ook interne en externe audits (de werking, 2e en 3e verdedigingslinie)
- *Act:* het aanpassen en/of verbeteren van beheersmaatregelen en de organisatiebrede aanpak van informatiebeveiliging op basis van bovengenoemde evaluatie.



Het doorlopen van deze cyclus zorgt voor een adequate beheersing waarbij de organisatie aantoonbaar voldoet aan de BIO en is uitgewerkt in hoofdstuk 4.

2.6.5 Beheersmaatregelen

Het uitgangspunt is dat de organisatie zich committeert aan de Baseline Informatiebeveiliging Overheid (BIO) die is vastgesteld voor alle overheidslagen. De BIO is gebaseerd op de beheersmaatregelen van de internationale norm ISO27001, die deels nader zijn uitgewerkt in overheidsmaatregelen. Keuzes die binnen de organisatie worden gemaakt bij implementatie en aanpassing van de beheersmaatregelen, zoals die uit de BIO, zijn gebaseerd op een risicoafweging en worden proportioneel getroffen. Daarbij wordt onder andere rekening gehouden met de financiële mogelijkheden van de gemeente.

Voor de proportionele toepassing van maatregelen wordt gebruik gemaakt van een dataclassificatie. Daarmee kunnen beheersmaatregelen worden afgestemd op het risicoprofiel van de gegevens ten aanzien van de vertrouwelijkheid, integriteit en beschikbaarheid ("BIV") van de gegevens.

De organisatie houdt een overzicht (GAP-analyse gemeente Landsmeer) bij van de implementatie van de beheersmaatregelen uit de BIO. Wanneer gekozen wordt af te wijken van de BIO, wordt daarover besloten door het management van de gemeente Landsmeer. Conform de eisen van de BIO wordt, waar van toepassing en indien mogelijk, gebruik gemaakt van de standaarden van het Forum Standaardisatie van de Nederlandse Overheid (https://www.forumstandaardisatie.nl/open-standaarden). De organisatie werkt nauw samen met landelijke diensten voor gemeenten, zoals de Informatiebeveiligingsdienst (IBD). Zowel in het overkoepelend (strategisch) informatiebeveiligingsbeleid en aanvullende beveiligingsbeleidsdocumenten moet ook verankering plaatsvinden naar aanvullende wet- en regelgeving of specifieke onderwerpen zoals beveiliging van Procesautomatisering (PA) en IoT.

2.6.6 Incident Management Response en Bedrijfscontinuïteit

Uitgangspunten:

- De verantwoordelijkheden ten aanzien van incidentmanagement en bedrijfscontinuïteit zijn vastgesteld en belegd.
- Incidenten worden geclassificeerd op basis van ernst, aard en (potentiële) impact. Afhankelijk van deze classificatie wordt een bijbehorende crisisteam-samenstelling geactiveerd.
- Er is een procedure vastgesteld voor het melden en afhandelen van beveiligingsincidenten en datalekken.
- Indien het incident de continuïteit of veiligheid van essentiële digitale diensten in gevaar brengt, geldt (op grond van NIS2) een meldplicht. Dan wordt, met ondersteuning van de IBD, **binnen 24 uur** een melding gedaan bij de Rijksinspectie Digitale Infrastructuur (RDI), inclusief aard, (vermoedelijke) oorzaak, impact en getroffen/voorgenomen maatregelen.
- De draaiboeken van kritieke processen worden regelmatig geoefend. Bevindingen en leerpunten worden vastgelegd en, indien nodig, gebruikt om de draaiboeken en het incidentmanagementproces te verbeteren en te actualiseren; de resultaten worden gerapporteerd aan het management. Het incidentmanagementproces wordt periodiek geëvalueerd en zo nodig geactualiseerd.
- Alle beveiligingsincidenten worden geregistreerd en gemeld in TOPdesk en bijgehouden in het register van beveiligingsincidenten en datalekken.

Voor interne crisisbeheersing beschikt de gemeente Landsmeer over een Bedrijfscontinuïteitsteam (BCT). Dit team komt samen bij grote incidenten of calamiteiten die een ernstige verstoring van informatiesystemen of processen veroorzaken. Het BCT bepaalt in welke gevallen, en door wie, contact wordt onderhouden met externe autoriteiten (zoals brandweer, toezichthouders of IBD). De handels- en werkwijze bij dergelijke situaties zijn vastgelegd in het Bedrijfscontinuïteitsplan van de gemeente Landsmeer. Voor alle kritieke processen zijn specifieke draaiboeken beschikbaar. Het BCT bestaat minimaal uit de gemeentesecretaris (voorzitter), CISO, TISO, privacy officer/FG, proceseigenaar (teammanager), adviseur crisisbeheersing, communicatieadviseur/woordvoerder, relevante experts (indien nodig) en een notulist. De burgemeester beslist of opschaling naar het GBT of de veiligheidsregio noodzakelijk is.

2.6.7 Verantwoording met ENSIA

De gemeente legt jaarlijks verantwoording af over informatiebeveiliging via de ENSIA-systematiek[5]. Hiervoor wordt een ENSIA-coördinator aangewezen. Deze coördineert het verzamelen van de benodigde informatie bij de verantwoordelijke teammanagers en medewerkers, zodat de jaarlijkse ENSIA-vragenlijsten volledig kunnen worden ingevuld. De verantwoording wordt opgenomen in het jaarverslag via de ENSIA Collegeverklaring Informatiebeveiliging. In deze verklaring geeft het college van B&W aan in hoeverre de gemeente voldoet aan de afspraken van de ENSIA-verantwoording en de wettelijke eisen, zoals de AVG. Tevens worden eventuele verbetermaatregelen benoemd. De ingevulde zelfevaluatie vormt de basis voor de collegeverklaring aan de raad. Via ENSIA legt de gemeente daarnaast verantwoording af aan de stelselhouders voor DigiD, BGT, BRO, BAG en SUWI.

Middels deze verantwoording worden het college en de gemeenteraad van de gemeente Landsmeer geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Landsmeer informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

2.6.8 Externe partijen en ketenpartners

De gemeente Landsmeer verlangt van externe partijen zoal IT-leveranciers, verbonden partijen en ketenpartners, zoals zorginstellingen binnen het sociaal domein, dat zij aantoonbaar voldoen aan een vergelijkbaar niveau van informatiebeveiliging als vastgelegd in de BIO. Deze eisen worden vastgelegd in juridische afspraken, zoals verwerkers- en samenwerkingsovereenkomsten, waarin de verantwoordelijkheden en verplichtingen op het gebied van informatiebeveiliging expliciet zijn opgenomen en juridisch afdwingbaar zijn. Om naleving te borgen voert de gemeente regelmatig risicoanalyses uit, worden jaarlijks verantwoordingsrapportages opgevraagd en wordt via een robuust systeem van verantwoording en controle toegezien op de naleving van de afgesproken maatregelen.

2.6.9 Bewustwording

Medewerkers vormen een essentiële schakel bij het voorkomen van informatiebeveiligingsincidenten en datalekken. Daarom worden bewustwordingsprogramma's en trainingen ingezet om hen inzicht te geven in hun rol, risico's en dreigingen, en om hen in staat te stellen hier adequaat op te reageren. Indien het beleid of beheersmaatregelen eisen stellen aan taken en verantwoordelijkheden, worden deze vastgelegd in functieafspraken. Elke medewerker – vast, tijdelijk, intern, extern of (keten)partner, is verplicht gegevens en applicaties te beschermen tegen ongeautoriseerde toegang, wijziging, openbaar-

5) ENSIA staat voor Eenduidige Normatiek Single Information Audit. Middels ENSIA verantwoorden gemeenten zich over informatiebeveiliging en kwaliteit.

making, vernietiging of overdracht. (Vermeende) inbreuken moeten direct bij de helpdesk worden gemeld. Van iedere medewerker wordt verwacht dat hij of zij de gedragsregels kent, naleeft en eigen verantwoordelijkheid neemt binnen het vastgestelde beleid en normenkaders.

3. Organisatie, taken & verantwoordelijkheden

3.1 Bestuurlijke context

Het college van B en W is eindverantwoordelijk voor de informatieveiligheid, daarmee in het bijzonder de portefeuillehouder (burgemeester). Collegeleden zijn integraal verantwoordelijk voor hun portefeuilles inclusief informatieveiligheid en privacy. Het college bewaakt of de gemeentelijke informatiebeveiligingsdoelstellingen worden/zijn gerealiseerd door de gemeente Landsmeer. In die hoedanigheid stelt zij het strategisch informatiebeveiligingsbeleid vast, waarin wordt aangegeven hoe zij met die verantwoordelijkheid wil omgegaan.

Dit Strategisch Informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van de gemeente. De bestuurders en management geven sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

3.2 Ambtelijke organisatie

De gemeentesecretaris van de gemeente Landsmeer is ambtelijk eindverantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid. Het management geeft invulling aan die verantwoordelijkheid door het omzetten van het beleid in doelstellingen en plannen, de integratie daarvan in de processen van de organisatie, toewijzing van rollen en verantwoordelijkheden, het ter beschikking stellen van middelen, het bekendmaken van het beleid en het belang daarvan, het aansturen en ondersteunen van medewerkers bij en het toezien op uitvoering van het beleid, evaluatie en bijstelling van de aanpak van informatiebeveiliging en beheersingsmaatregelen. De CISO rapporteert namens het management gevraagd en ongevraagd aan respectievelijke portefeuillehouder. Daarnaast rapporteer de CISO namens het management over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. Verbeterplannen maken onderdeel uit van de reguliere P&C cyclus in de lijn.

In de ambtelijke eindverantwoordelijkheid wordt de gemeentesecretaris ondersteund door de organisatie, namelijk door:

Medewerkers

Iedere medewerker is zelf verantwoordelijk voor het uitvoeren van het informatiebeveiligingsbeleid als onderdeel van hun professionele verantwoordelijkheid. Om hen daarbij te ondersteunen is er een "Gedragscode Informatiebeveiliging en Privacy", waarin gedragsregels staan voor medewerkers. Ook worden medewerkers bewust gemaakt van hun rol/bijdrage en worden zij geïnformeerd over hoe zij deze rol en/of bijdrage kunnen uitvoeren. Dit gebeurt zowel bij indiensttreding als op basis van regelmatige bewustwordings- en leerinterventies. Daarvoor wordt een bewustwordingsprogramma opgesteld door de CISO.

Teammanagers/proceseigenaren

Teammanagers zijn verantwoordelijk voor:

- de uitvoering van het informatiebeveiligingsbeleid en beheersmaatregelen binnen hun team. Informatiesystemen die door meerdere organisatieonderdelen worden gebruikt vallen onder de verantwoordelijkheid van de door het management aangewezen systeemeigenaar;
- het zorgen voor een adequate inrichting van werkprocessen en aansturing van medewerkers;
- het toezien op de naleving van het beleid en het bevorderen van het beveiligingsbewustzijn;
- het uitvoeren van onderdelen van beheersmaatregelen, zoals (het bevestigen van) de dataclassificatie voor processen en applicaties van het team of het beoordelen van toegangsrechten;
- het (laten) uitvoeren van risicoanalyses en (pre)DPIA's voor de processen waar zij verantwoordelijk voor zijn;
- Het vaststellen, documenteren en actualiseren van relevante wettelijke, statutaire, regelgevende en contractuele eisen voor hun informatiesystemen;
- Het uitvoeren van processpecifieke borgings-/controleactiviteiten, vaak samenhangend met processpecifieke applicaties;
- Het uitvoeren van processpecifieke beheersmaatregelen, bijvoorbeeld voortvloeiend uit wetgeving. Bijvoorbeeld over basisregistraties, waardedocumenten zoals reisdocumenten/rijbewijzen, DigiD en SUWI;
- Het nemen van maatregelen om beveiligingsincidenten binnen hun team te voorkomen;
- Het vroegtijdig betrekken van de CISO en de juridische privacy adviseurs bij nieuwe of gewijzigde processen.

Beveiligingsbeheerders informatiebeveiliging

Teammanagers kunnen beveiligingsbeheerders benoemen, die hen ondersteunen bij het uitvoeren van de bovengenoemde taken. Op welk niveau van de organisatie de benoeming van een contactpersoon wenselijk is hangt af van de omvang van het team en de hoeveelheid gevoelige gegevens die daarin wordt verwerkt. Onder de taken van een contactpersoon vallen het signaleren van beveiligingsissues binnen het team, het aanleveren van rapportage informatie aan de CISO en/of Privacy Officer, informatieverzameling voor DPIA's en het bevorderen van het bewustzijn binnen het team. De contactpersonen zijn aanspreekpunt bij audits, zoals ENSIA. De teammanager behoudt de eindverantwoordelijkheid.

Beveiligingsbeheerder
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid binnen een specifiek deelgebied. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de beveiligingsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan de zogenoemde beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: DigiD, BRP, reisdocumenten en rijbewijzen (officieel beveiligingsfunctionaris reisdocumenten en rijbewijzen)., en de BAG, BGT en BRO. Daarnaast worden er (indien mogelijk) beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals facilitaire zaken, ICT, DIV (archivering) en personeelszaken) en de primaire processen (bijvoorbeeld sociaal domein, financiën, openbare orde en veiligheid, dienstverlening (eventueel gecombineerd met BRP en waardedocumenten), ruimte/omgeving).

Specifiek verplichte beveiligingsbeheerdersrollen:
- *Beveiligingsfunctionaris reisdocumenten- en rijbewijzen:* verantwoordelijk voor het beheer van en het toezicht op de naleving van de beveiligingsprocedures Waardedocumenten. Deze functie is vastgelegd en beschreven in de functiebeschrijving waardedocumenten.
- *Beveiligingsbeheerder BRP:* verantwoordelijk voor de inrichting, organisatie en uitvoering van het informatieveiligheidsbeleid voor de gemeentelijke voorziening van de BRP. Deze functie is vastgelegd en beschreven in de Regeling beheer en toezicht Basisregistratie Personen (BRP) van Gemeente Landsmeer.
- *Beheerders van basisregistraties:* Voor elke basisregistratie waarvan Gemeente Landsmeer bronhouder is, draagt een beheerder de verantwoordelijkheid voor het inwinnen en bijhouden van de authentieke en niet-authentieke gegevens in een basisregistratie en voor het borgen van de kwaliteit van die gegevens. De beveiligingsbeheerder is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden.

CISO
De Chief Information Security Officer (CISO) is - vanuit een onafhankelijke rol/positie – verantwoordelijk voor:
- het opstellen, uitvoeren, evalueren en bijstellen van het beleid en de coördinatie van de jaarlijkse verbetercycli;
- het coördineren van de implementatie, uitvoering en borging van beheersmaatregelen;
- het toezicht houden op de uitvoering van het beleid in de lijn;
- het periodiek (1 keer in het kwartaal) rapporteren over de uitvoering van het beleid, actieplan informatiebeveiliging en over beveiligingsincidenten;
- het rechtstreeks rapporteren aan het management;
- het beheren en continu verbeteren van het Information Security Management System (ISMS);
- het bewaken van de PDCA-cyclus (plan–do–check–act) voor informatiebeveiliging binnen de organisatie;
- gevraagd en ongevraagd adviseren over informatiebeveiliging in brede zin;
- het bevorderen van het beveiligingsbewustzijn in de gehele organisatie;
- het (laten) uitvoeren van risicoanalyses en het bewaken van de voortgang van mitigerende maatregelen;
- het onderhouden van contacten met externe toezichthouders, auditors en ketenpartners omtrent informatiebeveiliging;
- het toetsen van nieuwe projecten, systemen en aanbestedingen op informatiebeveiligingsaspecten;
- het signaleren van relevante ontwikkelingen op het gebied van wet- en regelgeving en dreigingen, en deze vertalen naar beleid en maatregelen.

ISO
De Information Security Officer (ISO) is verantwoordelijk voor:
- ondersteuning en vervanging van de CISO

- op operationeel niveau gevraagd en ongevraagd adviseren en ondersteunen bij de uitvoering van het informatiebeveiligingsbeleid en jaarplan;
- de implementatie en uitvoering van beheersmaatregelen, zoals het beoordelen van kwetsbaarheden en het bevorderen van het veiligheidsbewustzijn;
- het registreren van beveiligingsincidenten in een incidentenregister en het coördineren van de afhandeling en evaluatie hiervan;
- het uitvoeren van risicoanalyses en het bewaken van de opvolging van verbetermaatregelen;
- het toetsen van projecten en wijzigingen op informatiebeveiligingsrisico's;
- het coördineren van IT-accountantscontroles (in samenwerking met de auditfunctie);
- het coördineren van ENSIA;
- het opstellen van tactische beleidsstukken en procedures.

TISO
De Technical Information Security Officer (TISO) is de spil tussen de CISO en de systeembeheerders en zorgt voor interactie en afstemming op het gebied van ICT beveiliging. Ook fungeert de TISO als gesprekspartner voor de CISO's van de partnergemeenten en adviseert hen zo nodig op gebied van technische beveiligingsvraagstukken.

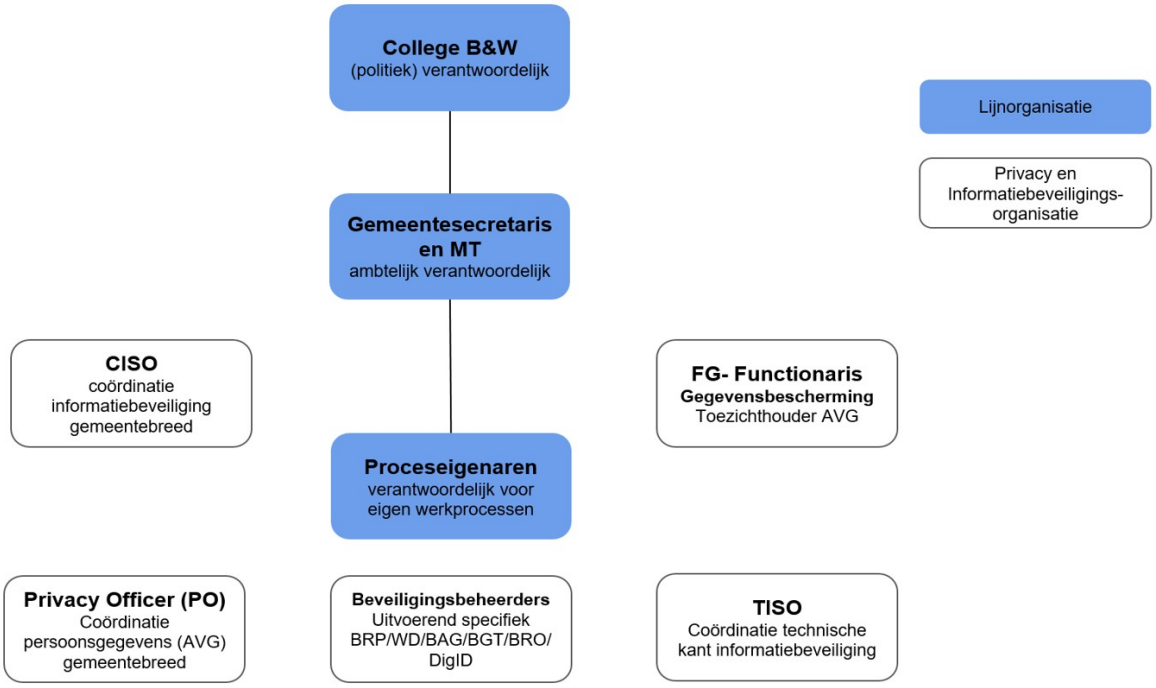
De *TISO* is verantwoordelijk voor:
- de implementatie van de technische informatieveiligheidsmaatregelen uit de BIO;
- het coördineren van ICT-technische beveiligingsincidenten (o.a. SIEM/SOC meldingen, DDOS-aanvallen, phishing, inbreuk infra), inclusief IBD meldingen, en afstemming hierover met de ISO;
- het inspelen op ontwikkelingen op het gebied van informatieveiligheid. Deze ontwikkelingen vertaalt hij naar maatregelen om de weerbaarheid van IT- infrastructuur te waarborgen;
- het richting geven aan het doorvoeren van updates bij ICT-technische beveiligingsincidenten;
- gevraagd en ongevraagd advies geven ter verbetering van de technische informatieveiligheid;
- het periodiek rapporteren aan de CISO over beveiligingsincidenten en de realisatie en effectiviteit van de beveiligingsmaatregelen en zaken of ontwikkelingen die bedreigend kunnen zijn voor de informatieveiligheid;
- het begeleiden van de technische werkzaamheden binnen audits en zelfevaluaties (BIO- maatregelen) en bewaakt de voortgang van de acties/bevindingen hieruit (Pentesten, ENSIA en IT-accountantscontrole) in afstemming met de teammanager ICT;

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG), die houdt toezicht, geeft kaders aan, informeert en adviseert vanuit zijn/haar wettelijke taak conform de AVG en de Wet politiegegevens (Wpg) en rapporteert hierover aan het management en is tevens bevoegd om rechtstreeks verslag te doen aan de gemeentesecretaris en het dagelijks bestuur van de gemeente Landsmeer.

Privacy Officer
Deze functie is gericht op de uitvoering en de naleving van de Algemene verordening gegevensbescherming (AVG) en de Wpg. De privacy officer adviseert alle lagen van de gemeente over privacybescherming, privacyvraagstukken en over activiteiten ter bescherming van persoonsgegevens. Zo adviseert en ondersteunt de privacy officer onder meer over het uitvoeren van Data Protection Impact Assessments (DPIA), op te stellen beleid, regelingen of verklaringen en het verwerken van persoonsgegevens. Ook is de privacy officer verantwoordelijk voor het afhandelen van verzoeken van rechten van betrokkenen, het melden van datalekken bij de Autoriteit persoonsgegevens en het vergroten van het privacy bewustzijn binnen de gemeente door het geven van interne trainingen.

Concernstaf
De stafteam Concerncontrol is verantwoordelijk voor:
- het coördineren van interne audits, bijvoorbeeld de Verbijzonderde Interne Controles (VIC) en het onderzoeksplan doelmatigheid en doeltreffendheid op basis van art. 213a van de Gemeentewet;
- het coördineren van externe audits, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening.

Andere medewerkers
Andere medewerkers die verantwoordelijk zijn voor specifieke onderdelen van het beleid, zoals het uitvoeren van specifieke beveiligingsmaatregelen en de bewaking daarvan. Deze specifieke taken en verantwoordelijkheden worden benoemd in de beschrijving van de beheersmaatregelen van de BIO.



Figuur 1. Functies en rollen in informatieveiligheidsorganisatie

3.3 Griffie
De griffier van de gemeenteraad van de gemeente Landsmeer is ambtelijk eindverantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid binnen de griffie, waarbij zo veel mogelijk gebruik wordt gemaakt van de faciliteiten van de gemeente en de beveiligingsmaatregelen die door de ambtelijke organisatie zijn getroffen.

De griffier vervult ook de rol van proceseigenaar, zoals in de vorige paragraaf beschreven, hetgeen onder andere betekent dat zij in die rol de autorisaties binnen applicaties met gegevens van de griffie en de raad bepaalt. De CISO en de FG van de gemeente zijn of worden tevens aangewezen voor de raad en de griffie. Medewerkers van de griffie hebben dezelfde in de vorige paragraaf beschreven taken ten aanzien van informatiebeveiliging als medewerkers van de ambtelijke organisatie.

4. De aanpak van informatiebeveiliging
4.1 Jaarcyclus
Om de borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, doorloopt de gemeente Landsmeer de onderstaande Plan, Do, Check, Act (PDCA) cyclus, zowel organisatiebreed als per beheersmaatregel, resulterend in een Information Security Management System (ISMS).

Het ISMS wordt toegepast in aansluiting bij (bestaande) bestuurs- en P&C-cycli en is onder te verdelen in:

Plan:
Voor ieder jaar wordt een actieplan opgesteld met verbeterpunten. Hierbij wordt rekening gehouden met de organisatiestrategie en -doelstellingen, risico's, regelgeving, de stand van de techniek en beschikbare middelen.

In het jaarlijks op te stellen actieplan Informatiebeveiliging (vast te stellen door het management) worden onderhouds- en verbeterslagen gepland en vastgesteld. Dit wordt gedaan op basis van input van teammanagers, de CISO, het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten, het Cybersecuritybeeld Nederland, de uitkomsten van audits (o.a. ENSIA en IT audit) en de standaarden waaraan de gemeente moet voldoen, zoals de BIO, AVG, Wpg, CSIR en op termijn de Wbni/NIS2.

In het jaarplan staan de acties en de planning vermeld, om het beleid stapsgewijs te implementeren en in praktijk te brengen.

Het jaarplan voor informatiebeveiliging wordt opgesteld op basis van:

- evaluatie van de uitvoering en resultaten van het vorige verbeterplan;
- risicoanalyse t.a.v. informatiebeveiliging op basis van de separaat beschreven aanpak voor risicoanalyse die het identificeren, analyseren/beoordelen, evalueren en het nemen van maatregelen omvat;
- evaluatie van de implementatie van beheersmaatregelen ten opzichte van de BIO (GAP-analyse);
- informatiebeveiligingsincidenten;
- trends ten aanzien van bedreigingen, kwetsbaarheden en technologische mogelijkheden en maatschappelijke ontwikkelingen;
- het informatiebeveiligingsbeleid en evaluatie van de naleving daarvan;
- de strategie en doelstellingen van de organisatie.

Het plan bevat meetbare doelen en een activiteitenplanning met verantwoordelijken, benodigde middelen, tijdslijnen en resultaten.

Do:
Het jaarplan en beheersmaatregelen worden uitgevoerd, waarbij beveiligingsmaatregelen worden ingevoerd en stapsgewijs worden verbeterd. De uitvoering van het jaarplan en de beheersmaatregelen wordt bewaakt. De CISO rapporteert daarover elk kwartaal aan het management. Waar nodig worden er aanvullende maatregelen genomen.

Check:
Borgings-/controleacties worden uitgevoerd om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd en of zij effectief zijn. De borgings-/controle acties worden opgenomen in een controleplan, zodat alle geïmplementeerde maatregelen passend worden afgedekt. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals kwetsbaarheidsanalyses/-scans en penetratietesten zijn onderdeel van dit controleplan. De CISO rapporteert hierover elk kwartaal aan het management.

Jaarlijks wordt een intern controleplan opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben.

Act:
Wanneer er afwijkingen van plannen of beheersmaatregelen optreden, of wanneer zich nieuwe ontwikkelingen voordoen (bijvoorbeeld in de maatschappij, wet- en regelgeving of techniek), wordt hierop bijgestuurd. Dit kan leiden tot het aanpassen van prioriteiten, het nemen van aanvullende maatregelen of het formuleren van aanbevelingen voor het volgende verbeterplan. Deze bijsturing vindt met name plaats binnen het managementteam, op basis van de adviezen van de CISO. Waar nodig worden besluiten genomen door het management of op bestuurlijk niveau. Op deze manier borgt de organisatie een continue verbetering van een passende informatiebeveiliging.

4.2 implementatie of vernieuwing van bedrijfsprocessen
Naast deze jaarlijkse cyclus wordt bij de implementatie of vernieuwing van bedrijfsprocessen de beveiliging van informatie geborgd. Het gaat daarbij bijvoorbeeld om de implementatie van nieuwe taken, werkprocessen of nieuwe (versies van) applicaties. De CISO en de Privacy Officer stellen daarvoor een proces op dat waarborgt dat nieuwe of vernieuwde bedrijfsprocessen voldoen aan het informatiebeveiligingsbeleid en dat de vereiste beheersmaatregelen daarvoor zijn geïmplementeerd. Dit proces bevat ten minste de volgende onderdelen:

- een dataclassificatie (zie bijlage 3), waarin de eisen aan vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens in het nieuwe of vernieuwde proces worden vastgesteld;
- een DPIA (Data Protection Impact Assessment, dan wel, Gegevensbeschermingseffectbeoordeling) wordt alleen uitgevoerd als deze verplicht is. De DPIA bestaat onder andere uit een analyse van risico's voor betrokkenen en een onderbouwing van de rechtmatigheid van de nieuwe verwerking van persoonsgegevens;
- bij een hoge dataclassificatie wordt een risicoanalyse uitgevoerd, tenzij deze al in het kader van een DPIA is of wordt uitgevoerd. In een risicoanalyse worden risico's geïdentificeerd en beoordeeld. Op basis daarvan beslist de proceseigenaar om een risico te accepteren, te beperken (te mitigeren), over te dragen (te verzekeren) of te vermijden (door de activiteit te staken), bijvoorbeeld door:
  - de keuze van passende maatregelen om de informatiebeveiligingsrisico's te beperken;
  - acceptatie van eventuele restrisico's door de directie;
  - bewaking van de uitvoering van de gekozen maatregelen ten aanzien van de risico's die in de DPIA of in de risicoanalyse zijn vastgesteld.

4.3 Evaluatie en herziening
Het Informatiebeveiligingsbeleid wordt jaarlijks op actualiteit en juistheid gecontroleerd door de CISO. Waar nodig worden addenda/amendementen ter besluitvorming voorgelegd.

Het Informatiebeveiligingsbeleid wordt ten minste elke vier jaar herzien op basis van:
- Een evaluatie van het beleid;
- Maatschappelijke ontwikkelingen en ontwikkelingen in de organisatiestrategie, wet- en regelgeving, de stand van de techniek en bedreigingen;
- Organisatiestrategie en -doelstellingen;
- Documentatie van de jaarlijkse verbetercycli (zie boven);
- Terugkoppeling van belanghebbende partijen, bijvoorbeeld de gemeenteraad en de ondernemingsraad;
- Onafhankelijke beoordelingen (audits);
- Aanbevelingen van relevante instanties, zoals toezichthouders (bijvoorbeeld de Autoriteit Persoonsgegevens), de VNG en de IBD.

5. Publicatie en wijzigingen

Dit document staat voor iedereen binnen de gemeente Landsmeer ter inzage op het intranet en wordt tevens gepubliceerd op overheid.nl. Dit document wordt periodiek geactualiseerd. De geactualiseerde versie wordt op het intranet gepubliceerd en de medewerkers worden daarop geattendeerd. De geactualiseerde versie wordt daarnaast ook gepubliceerd op overheid.nl.

Bijlage 1: Lijst met afkortingen

-	AVG	Algemene Verordening Gegevensbescherming
-	BAG	Basisregistratie Adressen en Gebouwen
-	BGT	Basisregistratie Grootschalige Topografie
-	BIO	Baseline Informatiebeveiliging Nederlandse Overheid
-	BRP	Basisregistratie Personen
-	CISO	Chief Information Security Officer
-	TISO	Technical Information Security Officer
-	CSIR	Cyber Security Implementatie Richtlijn
-	DAPI	Decentrale Aanspreekpunt voor Privacy en Informatiebeveiliging
-	DigiD	Beveiligde toegang tot overheidsdiensten
-	DPIA	Gegevensbeschermingseffectbeoordeling
-	ENSIA	Eenduidige Normatiek Single Information Audit
-	FG	Functionaris Gegevensbescherming
-	IBD	Informatiebeveiligingsdienst van de VNG
-	ISMS	Management systeem voor informatiebeveiliging
-	ISO	Information Security Officer
-	ISO	International Standards Organisation
-	NIS2	Europese richtlijn voor beveiliging van kritieke sectoren, die wordt omgezet in de Wbni
-	OT	Operational Technology, informatiesystemen voor de besturing van fysieke processen, zoals het gemeentelijke riool of verkeersregelinstallatie
-	PA	ProcesAutomatisering, zie OT
-	PNIK	onderdeel van regelgeving reisdocumenten
-	PO	Privacy Officer
-	PUN	Paspoortuitvoeringsregeling Nederland
-	Suwi	Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
-	UAVG	Uitvoeringswet AVG
-	VIC	Verbijzonderde Interne Controles
-	Wbni	Wet Beveiliging Netwerk- en Informatiesystemen, waarin de implementatie van de NIS2 richtlijn is opgenomen
-	WOO	Wet Open Overheid
-	Wpg	Wet Politiegegevens

Bijlage 2: DigiD-uitwerking norm B.01

In aanvulling op dit informatiebeveiligingsbeleid (dat integraal van toepassing is op al onze DigiD-aansluitingen) zijn voor DigiD de volgende aanvullende maatregelen en verantwoordelijkheden van toepassing:

Normen
- We conformeren ons aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD versie 3.0.
- Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor en CISO getoetst.
- Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

Eigenaarschap
- Geheel in lijn met de BIO is het eigenaarschap van de DigiD-webapplicaties (de webapplicaties die de DigiD-functionaliteit als module aanroepen) belegd in de lijnorganisatie en is de betreffende teammanager inwoners eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

Functioneel beheer
- Per DigiD-aansluiting is door de genoemde teammanager inwoners een functioneel beheerder iBurgerzaken aangewezen die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, controleren (middels een jaarlijkse TPM-verklaring) en bewijslast ervan op te bouwen in een auditdossier.
- Het auditdossier wordt jaarlijks aan onze externe auditor beschikbaar gesteld en bevat tenminste de contracten en servicerapportages van onze SaaS-leverancier(s) (norm B.05), de incidentprocedure en een overzicht van de incidenten (U/WA.02), de dataclassificatie (U/WA.05), bewijs dat de webapplicatie gehardend is (U/NW.06, tav DNSSEC) en de beoordeelde releases (C.08).
- Tweemaal per jaar (geagendeerd) wordt er door functioneel beheer beoordeeld of alle autorisaties compleet en actueel zijn; hierover wordt verslag (autorisatiematrix) gedaan richting verantwoordelijke teammanager inwoners.

Technisch
- Wij maken – voor wat betreft DigiD-aansluitingen - uitsluitend gebruik van cloudapplicaties die door SaaS-leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius afgekondigde normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse – door een onafhankelijk auditor opgestelde - TPM-verklaring verantwoording over aflegt.

Bijlage 3: Criteria Dataclassificatie

Classificatietabel			
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**
Geen / 0 **(geen schade)**	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de gemeentelijke website)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (MTD >1 maand) *(bv: ondersteunende tools als routeplanner)*
Laag / I **(Enige schade)**	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn (MTD 1 week tot 1 maand) *(bv: administratieve gegevens)*
Midden / II **(serieuze schade)**	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, BSN, financiële procesgegevens)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (MTD 2-7 dagen/1 week) *(bv: voorwaardelijke primaire proces informatie)*
Hoog / III **(zeer grote schade)**	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) ***(bv: gezondheids**-/medische gegevens, omvattende financiële gegevens (SUWI) en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke gemeentelijke informatie op de website o.a. waaraan rechten zijn te ontlenen)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (MTD max 2 dagen) *(bv: crisisbeheersing, basisregistraties, zoals BRP)*

Bron van bovenstaande tabellen: Handreiking Dataclassificatie, IBD, 2016 met aanvullingen door BMC