GEMEENTE Lansingerland

Strategisch informatiebeveiligings-beleid

GEMEENTE Lansingerland

Inhoudsopgave

Nadere informatie CISO
Team
Domein
Email ciso@lansingerland.nl
Telefoon 43 40
Postbus 1
2650 AA Lansingerland
www.lansingerland.nl

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid en vervangt het in 2020 vastgestelde 'Strategisch Informatiebeveiligingsbeleid gemeente Lansingerland 2020-2022' (T19.20329) Deze nota is richtinggevend en kaderstellend en wordt uitgewerkt in aanvullende, onderwerpspecifieke, beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit Strategisch gemeentelijk Informatiebeveiligingsbeleid zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op ontwikkeling die in de voorgaande jaren is ingezet. De basis voor dit strategisch beleid is de Baseline Informatiebeveiliging Overheid (BIO) en de implementatierichtlijnen uit NEN-ISO/IEC 27002. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de Vereniging Nederlandse Gemeenten (VNG) , Art. 32 van de Algemene Verordening Gegevensbescherming (AVG) voor de beveiliging van persoonsgegevens en de relevante artikelen uit de Wet Politiegegevens (Wpg).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet met ontwikkelingen, standaarden, positionering van het beleid en uitgangspunten. In hoofdstuk 3 wordt de organisatie en de verantwoordelijkheden rond informatiebeveiliging beschreven en in hoofdstuk 4 de aanpak van informatiebeveiliging, oftewel hoe daar concreet invulling aan wordt gegeven.

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 Lansingerland verstaan we de passende bescherming van vertrouwelijkheid, integriteit en beschikbaarheid ("BIV") van informatie die door of onder verantwoordelijkheid van de gemeente Lansingerland 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 het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Ambitie

In lijn met het coalitieakkoord en het werkprogramma College 2022-2026: een stabiele, beschikbare en veilige ICT-omgeving met een professionele organisatie is een randvoorwaarde voor het succes van de gemeente. Het is de ambitie van de gemeente om te voldoen aan relevante wet- en regelgeving. Nu en in de toekomst, zodat de dienstverlening van de gemeente beschikbaar is en blijft.
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 kwaadwillenden 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 Lansingerland 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 op het gebied van informatiebeveiliging 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

Uiterlijk 2024 zal de Europese "Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie" (NIS2 richtlijn) worden omgezet in de Wet Beveiliging netwerk- en informatiesystemen (Wbni). Deze wet wordt uiterlijk oktober 2024 van kracht. De NIS2 richtlijn stelt extra eisen aan vitale aanbieders, waaronder organisaties in de afvalwater-keten, zoals gemeenten met het gemeentelijke riool. De exacte eisen van de nieuwe Wbni zijn nog niet bekend, maar met de implementatie van de BIO bereidt de gemeente zich zo goed mogelijk voor op deze nieuwe richtlijn.

2.2.5 Kunstmatige intelligentie

Sinds 2022 zien we een snelle ontwikkeling van de toepassing van kunstmatige intelligentie. Dit vormt een bedreiging voor informatiebeveiliging, bijvoorbeeld doordat:

- het gebruik van kunstmatige intelligentie in chatbots, zoals ChatGpt of zoekmachines, zoals Bing, er toe kan leiden dat gevoelige informatie wordt gelekt en door de aanbieders wordt gebruikt.
- hackers kunstmatige intelligentie gebruiken, bijvoorbeeld voor het opstellen van overtuigende phishing mails en het kraken van wachtwoorden.

De gemeente voorziet in een richtlijn omtrent veilig gebruik van kunstmatige intelligentie. Kunstmatige intelligentie en phishing zijn onderdeel van de continue bewustwordingsactiviteiten om medewerkers te informeren over veilig gebruik en de risico's hiervan.

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 op het vlak van informatiebeveiliging. 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.

[1] **https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf**

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 27002:2012 genomen.
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 verkeersregelinstallaties, 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 beleidsafdelingen 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
- Cybercrisisplan
- Procedures informatieveiligheid (procedure antecedentenonderzoek, indiensttreding, overplaatsing medewerker en vertrek medewerker)
- Handout informatieveiligheid voor medewerkers
- Reglement gebruik digitale middelen
- Beveiligingsbeleid ICT
- Cryptografiebeleid
- Beveiligingsbeleid externe partijen (incl. leveranciers)
- BRP beveiligingsplan
- Suwi-net beveiligingsplan

Deze zijn beschikbaar via het intranet.

[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**

2.5 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, 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 aanvullende beleidsdocumenten 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 eindverantwoordelijke 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 Lansingerland uit van de volgende uitgangspunten.

2.6.1 Naleving

Het uitgangspunt is dat het College van B en W van de gemeente Lansingerland, de directie, de Chief Information Security Officer (CISO) en de proceseigenaren (lijnmanagers) 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

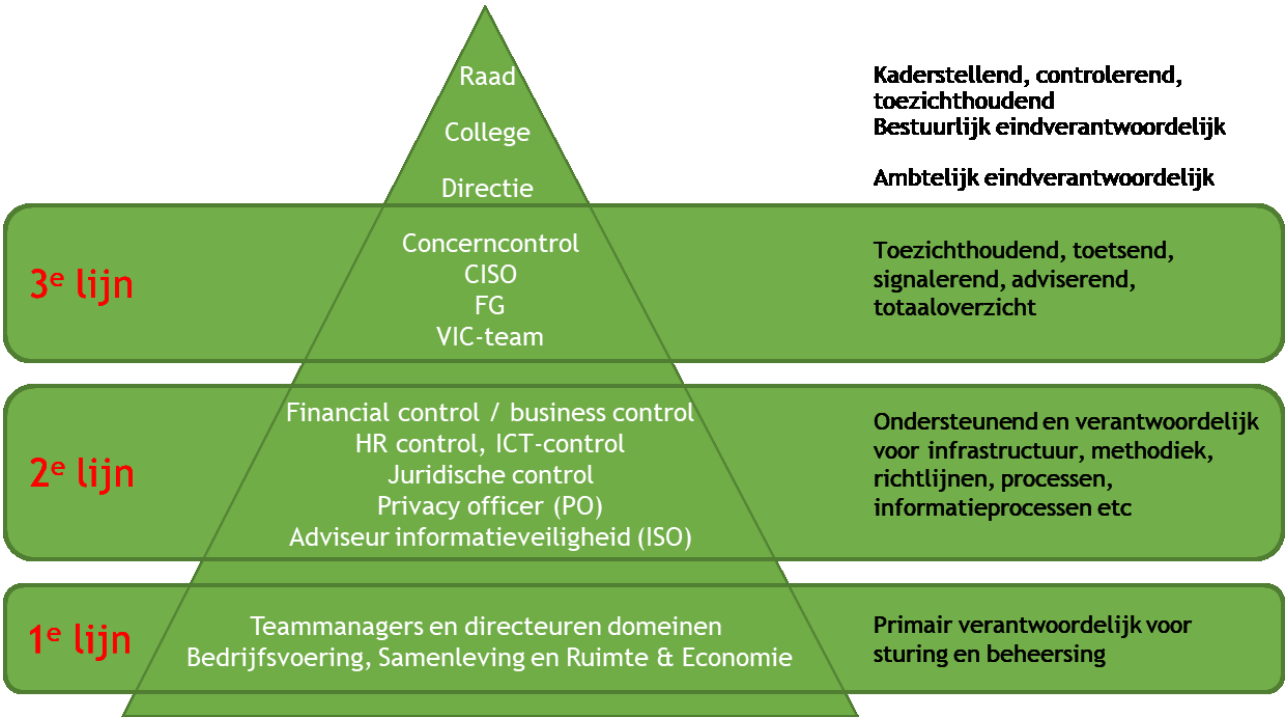
Het uitgangspunt is de toepassing van de Three lines of defense. Bij de toepassing van informatiebeveiliging staat het faciliteren van de werkprocessen van de organisatie voorop. Informatiebeveiliging dient hieraan een bijdrage te leveren door het veilig werken met informatie te faciliteren. Dat betekent 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 de directie.
De organisatie past daarvoor de drie verdedigingslijnen toe vanuit Interne Controle::

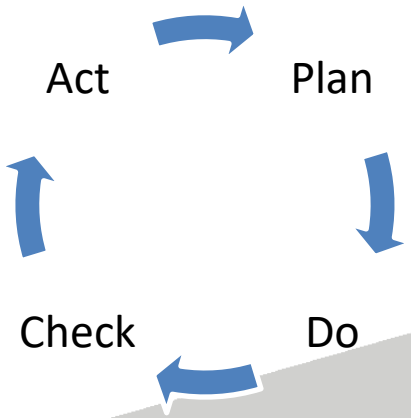
1) De beheersing van werkprocessen binnen de afdeling onder verantwoordelijkheid van de teams onder leiding van de teammanagers en directeuren. Dat wil zeggen: werkprocessen op orde, passende werkinstructies en werken volgens afspraken. Dat betekent dat de teams zelf 'in control' (lees, beheersing van 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[5], ISO en andere ondersteunende afdelingen met advies en hulpmiddelen voor beheersmaatregelen in de 1e lijn. Dit omvat ook hulpmiddelen voor en regie op voor borging/controle van beheersmaatregelen in de lijn, bijvoorbeeld door kwaliteitsfunctionarissen of teamleiders. 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 stafafdeling 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 directie, college en raad.

[5] In de huidige situatie. De organisatie streeft op termijn naar de positionering van de CISO in de 3e lijn.



2.6.3 Management systeem voor informatiebeveiliging (ISMS)

Het uitgangspunt is dat de gemeente Lansingerland 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 Lansingerland 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.

2.6.4 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 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 bij van de implementatie van de beheersmaatregelen uit de BIO.
Wanneer gekozen wordt af te wijken van de BIO, wordt daarover besloten door de directie van de gemeente Lansingerland.
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.

2.6.5 Verantwoording met ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek[6]. Dat betekent dat jaarlijks een ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teammanagers. De teammanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.
De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording informatiebeveiliging en wettelijke eisen zoals uit de AVG. Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegeverklaring aan de raad.
Via ENSIA verantwoordt de gemeente zich ook aan de stelselhouders voor DigiD/WOZ/BAG/SUWI.
Middels deze verantwoording worden het bestuur van de gemeente Lansingerland en de gemeenteraad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Lansingerland informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

2.6.6 Externe partijen

Het uitgangspunt is dat de gemeente Lansingerland verlangt van externe partijen dat zij aantoonbaar voldoen aan een vergelijkbaar niveau van informatiebeveiliging als de BIO, wanneer zij gegevens in opdracht

[6] **ENSIA staat voor Eenduidige Normatiek Single Information Audit. Middels ENSIA verantwoorden gemeenten zich over informatiebeveiliging en kwaliteit.**

van de organisatie verwerken en van ketenpartners waarmee gegevens van inwoners worden uitgewisseld. Het gaat daarbij bijvoorbeeld om IT-leveranciers, maar ook ketenpartners in bijvoorbeeld Wmo en Jeugdzorg, zoals zorginstellingen. Dit wordt gewaarborgd in juridische overeenkomsten, zoals verwerkersovereenkomsten.

2.6.7 Medewerkers

Medewerkers zijn een essentiële schakel in het voorkomen van informatiebeveiligingsincidenten en datalekken. Wanneer technische maatregelen falen of doorbroken worden, zijn medewerkers vaak nog in staat om een inbreuk te voorkomen. Daarom worden programma's uitgevoerd om medewerkers bewust te maken van hun rol, bedreigingen en risico's en worden zij getraind om hier adequaat op te reageren. Wanneer dit beleid en/of beheersmaatregelen eisen stellen aan taken en verantwoordelijkheden van medewerkers dan worden deze opgenomen in aanvullende individuele afspraken op functieniveau tussen de teammanager en de medewerker.
Iedere medewerker, zowel vast als tijdelijk, intern of extern, (keten)partner of betrokkene, is verplicht waar nodig gegevens en applicaties te beschermen tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of ongeautoriseerde overdracht. Bij (vermeende) inbreuken hierop dienen medewerkers dit te melden bij de servicedesk.
Iedere medewerker wordt geacht de gedragsregels van de organisatie te kennen en uit te dragen bij het uitoefenen van zijn of haar functie. We gaan uit van de eigen verantwoordelijkheid van medewerkers zowel vast als tijdelijk, intern of extern en overige betrokkene(n) voor hun gedrag binnen het vastgestelde beleid, de basisregels en geldende normenkaders.

3. Organisatie, taken en verantwoordelijkheden

3.1 Bestuurlijke context

Het College van Burgemeester en Wethouders is bestuurlijk eindverantwoordelijke voor de informatiebeveiliging die door de gemeente Lansingerland wordt uitgevoerd. Met andere woorden zij bewaakt of de gemeentelijke informatiebeveiligingsdoelstellingen worden/zijn gerealiseerd door de gemeente Lansingerland. In die hoedanigheid stelt zij het strategisch informatiebeveiligingsbeleid vast, waarin wordt aangegeven hoe zij met die verantwoordelijkheid wil omgegaan.
Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het bestuur van de gemeente. De bestuurders en directeuren geven sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

3.2 Ambtelijke organisatie

De directie van de gemeente Lansingerland is ambtelijk eindverantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid. De directie 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 de directie gevraagd en ongevraagd aan respectievelijke portefeuillehouders. Daarnaast rapporteer de CISO namens de directie 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 directie ondersteund door de organisatie, namelijk door:

Medewerkers
alle 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 handout “informatieveiligheid & privacy voor medewerkers” (T21.01745), waarin gedragsregels staan voor medewerkers. Ook worden medewerkers bewust gemaakt van hun rol/bijdrage en worden zij geïnformeerd over hoe zij deze kunnen rol en/of bijdrage kunnen uitvoeren. Dit gebeurt zowel bij indiensttreding als op basis van regelmatige bewustwordings- en leerinterventies. Daarvoor wordt jaarlijks een bewustwordingsprogramma opgesteld door de CISO

Proceseigenaren
Proceseigenaren 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 de directie aangewezen systeemeigenaar;

- het zorgen voor een adequate inrichting van werkprocessen en aansturing van medewerkers (1e linie zie paragraaf 2.6.2);
- 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 de afdeling 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 afdeling te voorkomen;
- Het vroegtijdig betrekken van de CISO bij nieuwe of gewijzigde processen.

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

CISO
De Chief Information Security Officer (CISO) is - vanuit een onafhankelijke rol/positie – verantwoordelijk voor:

- het opstellen, uitvoeren, evaluaten 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 per kwartaal) rapporteren over de uitvoering van het beleid en over beveiligingsincidenten;
- het rechtstreeks rapporteren aan de directie;
- gevraagd en ongevraagd adviseren over informatiebeveiliging in brede zin;
- het registreren van beveiligingsincidenten in een incidentenregister en het coördineren van de afhandeling en evaluatie hiervan;
- het bevorderen van het beveiligingsbewustzijn in de gehele organisatie;
- het coördineren van de activiteiten van de ISO's en de privacy ambassadeurs.

ISO
De Information Security Officer (ISO) is verantwoordelijk voor:

- 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, de afhandeling en evaluatie van incidenten en het bevorderen van het veiligheidsbewustzijn;
- het coördineren van ENSIA.

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

Concernstaf
de stafafdeling 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 en interne audits op basis van art. 33 van de Wet Politiegegevens;
- het coördineren van externe audits, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening en de externe audit op basis van art. 33 van de Wet Politiegegevens.

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.

3.3 Griffie

De griffier van de gemeenteraad van de gemeente Lansingerland 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 teamleider/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 de 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 Lansingerland 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 plan 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 jaarplan Informatiebeveiliging (vast te stellen door de directie) 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 ENSIA en de standaarden waaraan de gemeente moet voldoen, zoals de BIO, AVG, Wpg, CSIR en op termijn de Wbni.
In het jaarplan staan de acties en de planning vermeld, om het beleid stapsgewijs in de praktijk om te zetten.

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 de directie. 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 directie.

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. Voor geïmplementeerde onderdelen van het ISMS en geïmplementeerde beheersmaatregelen wordt bepaald of en zo ja hoe deze worden opgenomen in het interne controleplan van de organisatie.

Op basis van rapportages van de CISO en uitkomsten van audits wordt de informatiebeveiliging geëvalueerd. Naar aanleiding van de uitkomsten worden besluiten genomen over de verbetering van het managementsysteem en beheersingsmaatregelen. Dit mondt uit in het jaarverslag. Daarin wordt in lijn met de P&C-cyclus en ondersteund door een In Control Verklaring (ICV) gerapporteerd over het doorlopen van de beschreven PDCA-cyclus met betrekking tot informatieveiligheid. In deze rapportage worden ook andere voor informatieveiligheid en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld.

Act:
Naar aanleiding van afwijkingen van plannen en beheersmaatregelen en andere ontwikkelingen, bijvoorbeeld in de maatschappij, wet- en regelgeving of techniek, wordt bijgestuurd, prioriteiten aangepast, aanvullende maatregelen genomen of aanbevelingen gedaan voor het volgende verbeterplan. Dit gebeurt met name in de directie op basis van de adviezen van de CISO. Waar nodig vindt besluitvorming door directie of op bestuurlijk niveau plaats. Daarmee zorgt de organisatie voor 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 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, 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 directieraad;
- 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 Contact met expertisegroepen

Specifieke informatie op het gebied van informatiebeveiliging, afkomstig van relevante expertisegroepen, leveranciers van hardware, software en diensten en de informatiebeveiligingsdienst voor gemeenten (IBD) wordt gebruikt om de informatiebeveiliging te verbeteren.

De organisatie heeft uitgewerkt met welke instanties contact wordt onderhouden en door wie. Dit overzicht wordt door de CISO beheerd en minimaal jaarlijks bijgewerkt.

4.4 Evaluatie en herziening

Het Informatiebeveiligingsbeleid wordt jaarlijks op actualiteit en juistheid gecontroleerd door de CISO en de FG. 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 medezeggenschapsraad;
- 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 Lansingerland ter inzage op het intranet en wordt op aanvraag ter beschikking gesteld aan andere belanghebbenden. Dit document wordt periodiek geactualiseerd. De geactualiseerde versie wordt op het intranet gepubliceerd en de medewerkers worden daarop geattendeerd.

Bijlagen

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
- 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: 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