Gemeente Landsmeer

GEMEENTEBLAD

Officiële uitgave van de gemeente Landsmeer

Nr. 112411

4 mei

2020

Informatiebeveiligingsbeleid 2019 - 2022 Gemeente Landsmeer

Voorwoord

Voor u ligt het strategisch informatiebeveiligingsbeleid voor de jaren 2019 - 2022 voor de gemeente Landsmeer en vervangt het in september 2014 vastgestelde informatiebeveiligingsbeleid.

Met dit *'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2019 - 2022'* zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn.

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 Informatiebeveiligingsplan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van:

√ de teammanagers;
√ de CISO;
√ het dreigingsbeeld van de IBD;
√ de uitkomsten van ENSIA.

Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

Wat is informatiebeveiliging?

Onder informatiebeveiliging (verder afgekort IB) wordt verstaan:

Het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid (BIV) van (persoons)gegevens en andere informatie.

Het juist omgaan met informatie is de verantwoordelijkheid van alle medewerkers van gemeente Landsmeer. Het is dan ook van belang dat alle medewerkers het beleid kennen en ernaar handelen. Het informatiebeveiligingsbeleid (verder afgekort IB-beleid) geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen. Het beperkt zich niet alleen tot de ICT en gaat over het politiek bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

Waarom informatiebeveiliging?

Informatie, waaronder privacygevoelige gegevens, is een van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt en die met minimale middelen maximale resultaten behaalt. De bescherming van vertrouwelijke en waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe vertrouwelijker of waardevoller de informatie is, hoe meer maatregelen er moeten worden getroffen.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar maakt bijvoorbeeld ook elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

Hoe is informatiebeveiliging geborgd?

Dit informatiebeveiligingsbeleid is de kapstok voor alle te nemen maatregelen in het kader van informatiebeveiliging. Uit de wet- en regelgeving waar de gemeente zich aan moet houden, vloeien maatregelen voort. Die maatregelen worden jaarlijks in de vorm van een informatiebeveiligingsjaarplan (met concrete acties) uitgewerkt en vervolgens uitgevoerd. Alle resultaten omtrent informatiebeveiliging worden in het Informatiemanagementsysteem (ISMS) van gemeente Landsmeer vastgelegd.

1. Inleiding

1.1 Het belang van informatieveiligheid

Informatie is één van de voornaamste bedrijfsmiddelen van gemeente Landsmeer. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar kan daarnaast ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke gevolgen.
Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

1.2 Visie

De komende jaren zet de gemeente Landsmeer in op het implementeren en borgen van noodzakelijke maatregelen met betrekking tot privacy, informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie.
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken. De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

1.3 Doelstelling

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.

Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks bij te stellen *'Gemeentelijk Informatiebeveiligingsplan*[1]*'*.

Doelstelling is het waarborgen van de continuïteit van de informatiesystemen en minimaliseren van gevolgen voortkomend uit incidenten. En binnen de wettelijke kaders ervoor zorgen dat gemeentelijke informatie adequaat wordt beheerd en beveiligd.

2. Strategisch beleid

2.1 Ontwikkelingen

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

Van BIG naar BIO

De BIO (Baseline Informatiebeveiliging Overheid)[2] is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG (Baseline Informatiebeveiliging Gemeenten).

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 (B), integriteit (I) en vertrouwelijkheid (V).

Het toekennen van classificatieniveaus aan data is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen.

1) Zie de volgende link:
https://www.informatiebeveiligingsdienst.nl/product/handreiking-bio-voor-kleine-gemeenten/
2) Zie de volgende link:
https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Verschillen tussen BIG en BIO
De BIO verschilt op een aantal punten van de BIG. De grootste verschillen zijn:
√ Minder maatregelen (bijna 60% minder);
√ Maatregelen zijn altijd verplicht;
√ Meer risicomanagement (het begint met een Baselinetoets BIO);
√ Drie Basisbeveiligingsniveaus (BBN)[3];
√ Selectie van ontbrekende maatregelen vooraf;
√ Toewijzing van maatregelen op eindverantwoordelijke;
√ Een baselinetoets die rekening houdt met die 3 niveaus.

Meer risicomanagement
De BIO legt meer nadruk op risicomanagement dan de BIG, die meer gaat over specifieke maatregelen. De rol van de bestuurder en teammanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. 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. Om daar invulling aan te geven wordt tegelijkertijd met de BIO een handreiking *'10 bestuurlijke principes voor informatiebeveiliging'*[4] van kracht. Deze principes ondersteunen bestuurders bij de invulling van hun verantwoordelijkheid.

Tien bestuurlijke principes voor informatiebeveiliging
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.

De 10 bestuurlijke principes voor informatiebeveiliging zijn:
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.

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.

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

2.2 Standaarden informatiebeveiliging
De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN- ISO/IEC 27002:2017 genomen. De interbestuurlijke werkgroep Normatiek heeft in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

3) Zie bijlage A
4) Zie de volgende link:
https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

2.3 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. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks bij te stellen *'Gemeentelijk Informatiebeveiligingsplan'*.

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

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af, zoals voor de BRP, PNIK en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.5 Strategische doelen
De strategische doelen van het informatiebeveiligingsbeleid zijn:
√ Het managen van de informatiebeveiliging;
√ Adequate bescherming van bedrijfsmiddelen;
√ Het minimaliseren van risico's van menselijk gedrag;
√ Het voorkomen van ongeautoriseerde toegang;
√ Het garanderen van correcte en veilige informatievoorzieningen;
√ Het beheersen van de toegang tot informatiesystemen;
√ Het waarborgen van veilige informatiesystemen;
√ Het adequaat reageren op incidenten;
√ Het beschermen van kritieke bedrijfsprocessen;
√ Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
√ Het waarborgen van de naleving van dit beleid.

2.6 Uitgangspunten
Het bestuur, de directie en het teammanagement spelen een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

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

Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
√ Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B&W is eindverantwoordelijke voor de informatiebeveiliging;
√ De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle informatiebronnen en -systemen die gebruikt worden door gemeente Landsmeer hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie;
√ Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening

organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses;
√ Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen hét managementsysteem van informatiebeveiliging (belegt in het ISMS);
√ De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid;
√ Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld;
√ Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
√ Het college van B&W stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast;
√ De directie stelt jaarlijks het informatiebeveiligingsplan vast;
√ De directie is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid;
√ De directie is verantwoordelijk voor het vragen om informatie bij de teammanagers en ziet erop toe dat de teammanagers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt;
√ De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie, voorafgaand aan de P&C-gesprekken;
√ Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen;
√ De teammanagers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
√ Hoewel de basisregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die gesteld zijn;
√ Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures;
√ Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie;
√ Teammanagers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben;
√ De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teammanagers voeren quick scans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.7 Randvoorwaarden
Belangrijke randvoorwaarden zijn:
√ De informatiebeveiliging maakt deel uit van afspraken met ketenpartners;
√ Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden;
√ Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
- de uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
- het dreigingsbeeld gemeenten van de IBD;
- de door de teammanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

2.8 Reikwijdte
√ Dit beleid is van toepassing is op alle gemeentelijke processen, op onderliggende informatiesystemen, op informatie en gegevens van de gemeente en op externe partijen; het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

√ Dit beleid is hét overkoepelende informatiebeveiligingsbeleid met een organisatiebrede werking, met als basis de BIO en waarbij voor bepaalde kerntaken op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen gelden. Zoals basisregistraties als de BRP en BAG, maar ook Suwinet, Paspoorten en ID-bewijzen PNIK, de archiefwet en de AVG.
√ Dit beleid is in lijn met het algemeen beleid uit de programma begroting van de gemeente en met de relevante landelijke en Europese wet- en regelgeving.

2.9 De BIO kort samengevat
√ De BIO geeft een ruime definitie voor een informatiesysteem, namelijk "een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie;
√ Het management is verantwoordelijk voor de beveiliging van informatie(systemen);
√ Informatiebeveiliging is een cyclisch proces volgens de Plan-Do-Check-Act cyclus;
√ Deze Plan-Do-Check-Act cyclus maakt het management verantwoordelijk voor het treffen van maatregelen op basis van risicomanagement;
√ De secretaris van gemeente Landsmeer is eindverantwoordelijk voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie;
√ Het management stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;
√ Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het management de maatregelen uit.

De BIO is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. Daarnaast concretiseert de BIO een aantal normen tot verplichte overheidsmaatregelen:
√ Op grond van wet- en regelgeving;
√ Vanwege de gemeenschappelijke veiligheid van informatieketens;
√ Omdat deze fundamenteel zijn voor een betrouwbare c.q. professionele informatievoorziening.

Informatiebeveiliging en privacy hebben een duidelijke relatie met elkaar, maar zijn wel twee verschillende disciplines. Het beleid omtrent privacy wordt in het Privacy Beleidskader (B&W besluit d.d. 23 juli 2019) beschreven en wordt hier buiten beschouwing gelaten. De focus ligt in dit document op het beveiligen van álle informatie van gemeente Landsmeer.

3. Organisatie, taken en verantwoordelijkheden
In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model:
√ Zijn de teammanagers verantwoordelijk voor de eigen processen;
√ Ondersteunt, adviseert en coördineert de tweede lijn (CISO, security officers) de teammanagers en bewaakt daarnaast ook of de teammanagers hun verantwoordelijkheden ook daadwerkelijk nemen;
√ Wordt in de derde lijn het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Aansturing: directie (secretaris)
De directie:
√ zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teammanager;
√ zorgt dat de teammanagers zich verantwoorden over de beveiliging van de informatie die onder hen berust;
√ zorgt dat de eindverantwoordelijke portefeuillehouder binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad;
√ stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast;
√ draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente;
√ autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in gemeente Landsmeer gezien als een integraal onderdeel van risicomanagement.

3.2 Uitvoering: teammanagers
Informatiebeveiliging valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. *Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wél.*

Alle processen, systemen, data, applicaties etc. dient altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teammanagers rapporteren aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg.

Taken van de teammanagers in het kader van informatiebeveiliging zijn:
- √ Het leveren van input voor wijzigingen op maatregelen en procedures;
- √ Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures;
- √ Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld;
- √ Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Voorbereiding en coördinatie van het overleg ligt bij de CISO.

3.3 Controle en verantwoording
Dit strategisch beleid is een verantwoordelijkheid van het bestuur van gemeente Landsmeer. De bestuurders van gemeente Landsmeer zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.4 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA- systematiek. 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 (of de medewerker aan wie deze werkzaamheden zijn gedelegeerd) 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&W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording Informatiebeveiliging. 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.

Bijlage A Basisbeveiligingsniveaus (deze bijlage behoort bij het Informatiebeveiligingsbeleid 2019-2022)

De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen *beschikbaarheid, integriteit en vertrouwelijkheid*. De BBN-toets helpt bij het kiezen van het best passende niveau. De beschikbaarheidsniveaus zijn gebaseerd op de geldende beschikbaarheidsniveaus die door de grote interne dienstenleveranciers worden gehanteerd. De vertrouwelijkheidsniveaus zijn in lijn gebracht met de schadescenario's die gelden voor de te beschermen belangen. De onderverdeling is als volgt:

	Beschikbaarheid	**Integriteit**	**Vertrouwelijkheid**
BBN 1	laag	laag	laag
BBN 2	midden	midden	midden
BBN 3	midden	midden	hoog

	BBN 1
Beschikbaarheid = laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/ gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: • Kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 28 uur; • maximale hersteltijd in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur) in 85% van de gevallen.
Integriteit = laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen.Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: • financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of • beperkt verlies van management control; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).
Vertrouwelijkheid = Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: • financiële gevolgen: op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; of • irritatie en ongemak bij burgers geventileerd in de media; of • interne negatieve publiciteit (imagoschade).
	BBN 2
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/ gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of

	• verlies van publiek respect; klachten van burgers; of • organisatiebrede negatieve publiciteit (imagoschade) of • significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • kantoorautomatisering en organisatie specifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatiebrede negatieve publiciteit (imagoschade) of • significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordings vragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of • bindende aanwijzing van de AP in verband met schending van de privacy; of • directe imagoschade, bijvoorbeeld door negatieve publiciteit.
	BBN 3
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: • politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatiebrede negatieve publiciteit (imagoschade); of • significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: • Kantoorautomatisering en organisatie specifi eke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; • maximaal dataverlies 24 uur; • maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld:

	• politieke schade aan een bestuurder: bestuurder moet zich verantwoorden n.a.v. verantwoordingsvragen; of • schade te herstellen door ambtelijke opschaling; of • financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of • belangrijk verlies van management control; of • verlies van publiek respect; klachten van burgers; of • organisatiebrede negatieve publiciteit (imagoschade) of • significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Hoog	Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; • informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of • aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of • weerstand tegen statelijke actoren is noodzakelijk.