Gemeente Geertruidenberg

Informatiebeveiligingsbeleid 2025-2028

Datum: 06-02-2025

Managementsamenvatting

De gemeente Geertruidenberg wil haar informatiebeveiliging goed op orde hebben. Toegankelijke en betrouwbare overheidsinformatie is essentieel om onze dienstverlening- en bedrijfsvoering processen uit te voeren. De wijze waarop Geertruidenberg haar informatiebeveiliging borgt staat in dit informatiebeveiligingsbeleid.

Normenkader & reikwijdte

Gemeenten zijn wettelijk verplicht om veilig met informatie om te gaan. De Baseline Informatiebeveiliging Overheid (BIO) van de VNG (Vereniging van Nederlandse Gemeenten) schrijft voor aan welke normen deze beveiliging moet voldoen. Het informatiebeveiligingsbeleid is gebaseerd op de BIO en omvat de bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van gemeente Geertruidenberg in de meest brede zin van het woord. Daarnaast dient de gemeente te voldoen aan de eisen van de Cyberbeveiligingswet (NIS2[1]), die specifiek is gericht op het waarborgen van cybersecurity van essentiële diensten.

Doelstelling

Dit informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen. Gemeente Geertruidenberg wil in control zijn en daarover op professionele wijze verantwoording af leggen. 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 applicaties.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het garanderen van de continuïteit en beschikbaarheid van informatie.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.
- Het waarborgen van de naleving van dit beleid.

Risicomanagement

De aanpak van informatiebeveiliging is 'risk based'. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is hierbij van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico's. Daarnaast dient de gemeente Geertruidenberg goed te zijn voorbereid op incidenten en crises. Risicomanagement is een gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en proactief te beheersen door het treffen van maatregelen. De 'risk-based' benadering betekent ook dat gefundeerd afgeweken kan worden van de baseline (BIO) indien gemeente Geertruidenberg hier een geaccepteerd risico loopt. Tegelijkertijd houdt dit in dat mogelijk meer maatregelen getroffen moeten worden ten opzichte van de baseline indien gemeente Geertruidenberg een onacceptabel hoog risico loopt.

[1] De Network and Information Security directive, of NIS2-richtlijn, is de opvolger van de NIS-richtlijn. Deze richtlijn is vastgesteld door de Europese Unie (EU) en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. Nederland heeft de NIS2-richtlijn vertaald naar de Cyberbeveiligingswet.

BIO

Om in control te zijn van informatiebeveiliging en te voldoen aan wet-, en regelgeving is de implementatie van die BIO vereist. De volgende stappen dienen hiervoor als basis te worden gehanteerd.

1. Verantwoordelijkheid en eigenaarschap over te beveiligen aspecten vastgelegd
2. Basisniveau voor beveiliging vastleggen (BBN[2]-analyse)
3. Status van informatiebeveiliging in kaart (GAP-analyse[3])
4. Selectie en toewijzing van controls & maatregelen aan eigenaar
5. Implementatie en borging maatregelen
6. Monitoring status van informatiebeveiliging en periodieke rapportage en sturing

Belangrijke rollen en verantwoordelijkheden

Het college van B&W en de directie zijn eindverantwoordelijk voor adequate informatiebeveiliging binnen gemeente Geertruidenberg, zoals ook is vastgelegd in de Cyberbeveiligingswet (NIS2). De clustermanagers zijn verantwoordelijk voor informatiebeveiliging binnen hun processen en de uitvoering van de maatregelen. De Chief Information Security Officer (CISO) heeft als taak informatiebeveiliging op een hoger niveau te brengen en het vervolgens structureel te laten borgen in de organisatie. Hierbij geeft de CISO gevraagd en ongevraagd advies. De Privacy Officer (PO) houdt zich bezig met privacyvraagstukken en de Functionaris Gegevensbescherming (FG) houdt toezicht op privacyaspecten. Verder dient elke medewerker integer om te gaan met informatieverwerking en zich te houden aan relevante wet-, en regelgeving.

[2] Een Basis Beveiligings Niveau (BBN) is een verzameling van een minimale set van passende maatregelen om een bepaald belang te beschermen. De BIO kent drie BBN's met bijbehorende beveiligingseisen, namelijk BBN1, BBN2, BBN3.

[3] Een GAP-analyse is een methode om een vergelijking te maken tussen een bestaande en een gewenste situatie.

Inhoud

Revisie

Dit beleidsdocument heeft een geldigheidsduur van *2025 tot en met december 2028.* Het is de bedoeling om dit beleidsstuk jaarlijks te herzien en waar nodig bij te werken.

1 Inleiding

1.1 Informatiebeveiliging

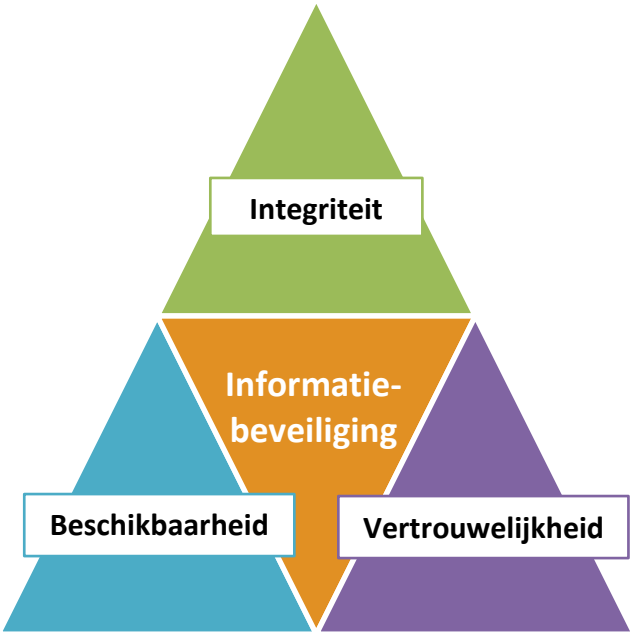
Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente om processen uit te voeren. Gemeenten beschikken over (zeer) vertrouwelijke informatie van zowel inwoners als bedrijven. Daarnaast zijn zij verantwoordelijk voor een betrouwbare en continue dienstverlening en bedrijfsvoering. Onze inwoners vertrouwen erop dat gemeente Geertruidenberg haar vertrouwelijke gegevens afdoende beveiligt.

Bij informatiebeveiliging is het belangrijk dat de juiste maatregelen, procedures en processen ervoor zorgen dat de beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid van informatie op het juiste niveau is beschermd. Voor het ene proces is vertrouwelijkheid van informatie belangrijker, voor het andere beschikbaarheid of integriteit. Mogelijk zijn alle aspecten van belang. Hieronder is weergegeven wat Gemeente Geertruidenberg verstaat onder deze begrippen.

Beschikbaarheid / continuïteit
Het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

Integriteit / betrouwbaarheid
Het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Vertrouwelijkheid / Exclusiviteit
Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.



Het informatiebeveiligingsbeleid is een overkoepelend beleidsstuk, waarbij in onderliggende plannen, documentatie, procedures en instructies verdere detaillering en afspraken zijn vastgelegd.

1.2 Scope

Dit beleid richt zich op alle gemeentelijke processen, systemen, en informatie, inclusief gebruik door medewerkers en partners, zowel lokaal als via cloud-oplossingen en uitbestede diensten. Gemeente Geertruidenberg heeft afspraken hieromtrent formeel vastgelegd met deze externe partijen. Naast de hoofdovereenkomst, vereist dit ook verwerkersovereenkomsten voor leveranciers die persoonsgegevens verwerken en dienstverlenersovereenkomsten (DVO's). Gemeente Geertruidenberg dient naleving van deze overeenkomsten periodiek te beoordelen zodat zij de betrouwbaarheid van informatieverwerking blijft borgen.

2 Informatiebeveiligingsbeleid

2.1 Visie gemeente Geertruidenberg

Een informatiebeveiligingsbeleid dient afgestemd te zijn op de (interne en externe) omgeving waarin het beleid wordt gebruikt, op de toekomst en op het beleid en de visie van de organisatie. In dit hoofdstuk wordt ingegaan op de visie van de Gemeente Geertruidenberg.

De komende jaren zet de gemeente Geertruidenberg verder in op het voldoen aan de gestelde informatiebeveiligingseisen (door Algemene Verordening Gegevensbescherming, BIO en NIS2), het verhogen van de informatiebeveiliging en de verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en is de basis voor het beschermen van belangen van inwoners en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel van de gemeente is hierbij betrokken.

De visie van de gemeente is om proactief risico's te identificeren en te beheersen, te voldoen aan wet- en regelgeving en het vertrouwen van inwoners in de gegevensbescherming te versterken door continue verbeteringen in onze aanpak.

2.2 Doelstelling

De gemeente Geertruidenberg wil informatiebeveiliging gestructureerd aanpakken om ervoor te zorgen dat de beveiliging op het juiste niveau is en blijft. Dit beleid beschrijft de gewenste situatie en doelstellingen volgens de geldende Baseline Informatiebeveiliging Overheid (BIO) en NIS2. Dit beleid is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en deze bescherming te waarborgen, waarbij risicomanagement als basis fungeert. Het beleid beschrijft ook de organisatie van informatiebeveiliging, inclusief rollen en verantwoordelijkheden en identificeert doelen gebaseerd op de BIO en de gemeentelijke visie. De gemeente Geertruidenberg wil in control zijn en daarover op professionele wijze verantwoording afleggen. In control betekent in dit verband dat de gemeente weet welke risico's zij loopt, welke maatregelen genomen zijn om deze risico's af te dekken en dat er een SMART[4]-planning is van de maatregelen die nog niet genomen zijn en dat dit verankerd is in een PDCA[5]-cyclus.

2.3 Uitgangspunten

Het management geeft een duidelijke richting aan informatiebeveiliging en toont betrokkenheid door het uitdragen en handhaven van het informatiebeveiligingsbeleid van de gemeente Geertruidenberg. De belangrijkste uitgangspunten van dit beleid zijn:

1. Alle gegevens en informatiesystemen zijn belangrijk voor de gemeente Geertruidenberg, bepaalde informatie is van vitaal en kritiek belang. Het college van B&W is eindverantwoordelijk voor informatiebeveiliging, in het bijzonder de portefeuillehouder voor informatiebeveiliging. De uitvoering van informatiebeveiliging is een verantwoordelijkheid van de clustermanagers;
2. Gemeente Geertruidenberg stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.

[4] SMART staat voor Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden. De SMART methode wordt gebruikt om doelstellingen die duidelijk, meetbaar, haalbaar en tijdgebonden zijn.

[5] PDCA staat voor Plan, Do, Check, Act. Het is een cyclus van continue verbetering die wordt gebruikt in kwaliteitsmanagement en procesverbetering. De PDCA-cyclus omvat het plannen van een verbetering, het uitvoeren van de geplande activiteiten, het controleren van de resultaten en het nemen van actie om verdere verbeteringen door te voeren.

3. De clustermanagers verantwoorden zich over de inrichting en de werking van informatiebeveiliging. Alle informatiesystemen die gebruikt worden door de gemeente Geertruidenberg hebben een proceseigenaar die de vertrouwelijkheid en/of waarde bepaalt van de gegevens die in het systeem zitten. De primaire verantwoordelijkheid voor de bescherming van deze gegevens ligt dan ook bij de proceseigenaar van de gegevens;
4. Wet- en regelgeving op het gebied van informatiebeveiliging en privacy dient te allen tijde te worden nageleefd. Dit kan tot gevolg hebben dat hieruit maatregelen ontstaan op het gebied van informatiebeveiliging.
5. De BIO is samen met de Cyberbeveiligingswet (NIS2) het voornaamste onderliggend kader. Gemeente Geertruidenberg stelt dit normkader vast waarbij er ruimte is voor risicoafweging en prioritering op basis van 'pas toe of leg uit'. De gemeente conformeert zich ook aan toekomstige wijzigingen in de BIO;
6. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
7. Door periodieke controle, organisatiebrede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt het fundament voor een betrouwbare informatievoorziening.
8. Regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid dienen te worden vastgelegd en vastgesteld, waarbij het college van B&W (rest)risico's met een (zeer) hoog risiconiveau ter acceptatie voorgelegd krijgen.
9. Medewerkers dragen bij aan informatiebeveiliging door beleid en procedures na te leven, incidenten te melden en een cultuur van informatiebeveiliging te bevorderen.

2.5 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging vormen een bestuurlijke aanvulling op het BIO normenkader en richten zich op de waarden die de bestuurder hanteert. Ze benadrukken de rol van het bestuur bij het waarborgen van informatiebeveiliging binnen de gemeentelijke organisatie en ondersteunen bij risicomanagement. 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.

3. Organisatie van informatiebeveiliging

Dit hoofdstuk gaat in op rollen en verantwoordelijkheden en op de borging van informatiebeveiliging. Een adequaat opgezette informatiebeveiliging vereist een governance-structuur waarin rollen en verantwoordelijkheden op het gebied van informatiebeveiliging zijn gedefinieerd en waarmee de besluitvorming, rapportage en escalatiestructuren met betrekking tot dit onderwerp zijn gereguleerd.

3.1 De gemeenteraad

De gemeenteraad is verantwoordelijk voor het beschikbaar stellen van middelen voor informatiebeveiliging en heeft tevens een controlerende rol op dit gebied. Het college legt jaarlijks verantwoording af aan de raad via het jaarverslag en een collegeverklaring, waarop een auditor Assurance verleent. Deze documenten zijn standaard onderdeel van de jaarlijkse ENSIA[6]-verantwoordingscyclus.

3.2 College B&W

Het college van burgemeester en wethouders is eindverantwoordelijkheid voor adequate beveiliging van informatie binnen de gemeente Geertruidenberg. Dit omvat:

a) Het vaststellen van het informatiebeveiligingsbeleid;
b) Het houden van toezicht op de uitvoering van het beleid, de stand van zaken, uitgevoerde plannen van het afgelopen jaar, en de planning van het komende jaar;
c) Het voorleggen van voorstellen aan de raad voor voldoende middelen om de informatiebeveiliging adequaat in te richten, en;
d) Het beoordelen van risico's en het expliciet nemen van besluiten over informatiebeveiliging.

3.3 Clustermanagers

Clustermanagers zijn verantwoordelijk voor het vaststellen van kaders en de implementatie van het informatiebeveiligingsbeleid binnen hun cluster. Ze hebben de bevoegdheid om processen te sturen en ervoor te zorgen dat deze voldoen aan het beleid, klantverwachtingen en bedrijfsdoelstellingen. Dit omvat het ontwerp en de inrichting van processen, evenals het nemen van maatregelen om risico's te beheersen, zelfs als deze plaatsvinden in andere teams of afdelingen waar zij proceseigenaar zijn.
Clustermanagers zorgen ervoor dat zij:

a) Sturen op bedrijfsrisico’s;
b) Rapporteren (via de CISO) rondom de relevante informatiesystemen over de voortgang van de planning, status van informatiebeveiliging, incidenten en andere ontwikkelingen.
c) Controleren of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
d) Beleidskaders (periodiek) evalueren en deze bijstellen waar nodig;
e) Een positieve en actieve houding hebben ten aanzien van informatiebeveiliging;
f) Een voorbeeldrol vervullen richting de medewerkers.
g) Waarborgen dat de medewerkers over voldoende kennis en kunde (blijven) beschikken ten aanzien van informatiebeveiliging om hun functie goed uit te kunnen voeren. Dit is inclusief digitale vaardigheden. De benodigde kennis en kunde kunnen per functie verschillen;
h) Sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
i) Rapporteren over compliance aan wet- en regelgeving en algemeen beleid.

[6] ENSIA (Eenduidige Normatiek Single Information Audit) is de verantwoordingsmethodiek voor informatieveiligheid en basisregistraties van gemeenten.

3.4 Chief Information Security Officer (CISO)

De CISO heeft als taak informatiebeveiliging op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelf verantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) uitvoeren en te adviseren over de bevindingen. Daarnaast rapporteert de CISO periodiek over de stand van zaken met betrekking tot informatiebeveiliging. De taken van de CISO op het gebied van informatiebeveiliging kunnen als volgt worden samengevat:

a) Opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;
b) Ondersteunt management bij het opstellen van informatiebeveiligingsrapportages en beoordeelt deze rapportages;
c) Periodiek rapporteren over de voortgang van de planning, status van informatiebeveiliging, incidenten en andere ontwikkelingen aan de portefeuillehouder;
d) Het inrichten van de informatiebeveiligingsorganisatie;
e) Afstemming van informatiebeveiliging met andere beveiligingsdomeinen.
f) Het uitvoeren van informatiebeveiligingsassessments;
g) Het toezien op naleving van de eisen voor informatiebeveiliging;
h) Het bevorderen van het informatiebeveiligingsbewustzijn van de hele organisatie;
i) De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's o.b.v. het dreigingsbeeld Nederlandse Gemeenten;
j) Het adviseren bij en begeleiden van informatierisicoanalyses;
k) Het coördineren en adviseren bij afhandelen van beveiligingsincidenten.
l) Indien het risico hierom vraagt, informeert en adviseert de CISO onverwijld de Algemeen Directeur in geval van overtreding of dreigende overtreding van wet- en regelgeving of richtlijnen van hogere organen. De CISO is bevoegd handelend op te treden en in te grijpen. De CISO legt achteraf verantwoording af over het handelend optreden.

3.5 Functionaris gegevensbescherming (FG)

De Functionaris Gegevensbescherming (FG) houdt zich bezig met het toezicht op alle privacyaspecten binnen gemeente Geertruidenberg. De functie is onafhankelijk van de lijn belegd en heeft de bevoegdheid om rechtstreeks naar de portefeuillehouder te rapporteren. De taken van de FG zijn:

a) Adviseren (zowel gevraagd als ongevraagd) over vraagstukken die te maken hebben met de omgang met persoonsgegevens;
b) Toezien op de naleving van de Algemene Verordening Gegevensbescherming (AVG) binnen de organisatie;
c) Het informeren van de organisatie betreffende de AVG;
d) Het zijn van een contactpunt voor betrokkenen (dit kunnen zowel inwoners als medewerkers zijn) m.b.t. de omgang met persoonsgegevens. De FG is daarbij gehouden aan geheimhouding;
e) Fungeren als aanspreekpunt voor datalekken binnen de organisatie;
f) Het coördineren van de afhandeling van datalekken conform de vastgestelde datalekprocedure;
g) Het eerste contactpunt met de Autoriteit Persoonsgegevens.

3.6 Privacy Officer

De Privacy Officer (PO) houdt zich bezig met alle privacyaspecten. Deze rol heeft de bevoegdheid om rechtstreeks naar het college van B&W en de directie te rapporteren. De taken van de PO zijn:

a) Zorgen dat de organisatie voldoet aan de formele (procedurele) en materiële eisen (uitvoering en inrichting) vanuit de privacy-gerelateerde wet- en regelgeving;
b) Adviseren (zowel gevraagd als ongevraagd) over vraagstukken die te maken hebben met de omgang met persoonsgegevens;
c) Het (laten) borgen van privacy-by-design in processen, projecten en veranderingen;
d) Toezien op de naleving van de privacy-gerelateerde wet- en regelgeving binnen de organisatie;
e) Het informeren van de organisatie betreffende de privacy-gerelateerde wet- en regelgeving en de impact op de bedrijfsprocessen;
f) Het creëren van privacy-bewustzijn;
g) Het zijn van een contactpunt voor betrokkenen (dit kunnen zowel inwoners als medewerkers zijn) m.b.t. de omgang met persoonsgegevens. De PO is daarbij gehouden aan geheimhouding;
h) Het afhandelen van datalekken conform de vastgestelde datalekprocedure.

3.5 ENSIA-coördinator

De verantwoording over informatiebeveiliging voor gemeenten gebeurt via het proces van ENSIA (Eenduidige Normatiek Single Information Audit). De ENSIA-coördinator is verantwoordelijk voor:

a) Het intern organiseren van ENSIA;
b) Het tijdig uitzetten van de zelfevaluatie vragenlijsten;
c) Het generen van rapportages vanuit de ENSIA-tool;
d) Het uploaden van verantwoordingsdocumenten;
e) Het meewerken aan het opstellen van de In Control Verklaring (ICV);
f) Het beheer van de ENSIA-tool.

3.6 Beveiligingsbeheerders

De beveiligingsbeheerders zijn verantwoordelijk voor het beheer, de coördinatie en het adviseren met betrekking tot de informatiebeveiliging binnen specifieke deelgebieden, zoals de Security Officer Suwinet, de beveiligingsbeheerder BRP en de beveiligingsfunctionaris voor reisdocumenten en rijbewijzen. Hun taken omvatten:

a) het implementeren en handhaven van maatregelen en procedures die voortvloeien uit het informatiebeveiligingsbeleid, inclusief maatregelen die gelden voor audit en zelfevaluatie vanuit de ENSIA-onderdelen;
b) het beheren van autorisaties.

3.9 De medewerkers

In zijn algemeenheid is iedere interne en externe (inclusief ingehuurde) medewerker in dit kader verplicht tot:

a) Het vertrouwelijk houden van informatie en wachtwoorden en andere vormen van toegangscodes in het bijzonder;
b) Het voldoen aan alle wettelijke verplichtingen;
c) Het conform interne regelgeving op veilige manier gebruiken van ICT-middelen;
d) Het gebruik van software in overeenstemming met de voorwaarden uit licentieovereenkomsten;
e) Het dusdanig omgaan met informatie en informatiemiddelen dat de beschikbaarheid, integriteit en betrouwbaarheid daarvan niet in gevaar komt;

f) Het voldoen aan het beleid en gedragsregels opgesteld door de gemeente.

Het geldt voor iedere medewerker dat het belang van gemeente Geertruidenberg vereist dat men oog heeft voor de wijze waarop collega's omgaan met informatie en dat incidenten op dit punt worden gesignaleerd.

3.10 Stuurgroep informatiebeveiliging en privacy

De stuurgroep informatiebeveiliging en privacy bestaat uit de CISO, de FG, de Controller, en indien nodig enkele managers en medewerkers van verscheidene afdelingen die een sleutelrol spelen betreffende informatiebeveiliging. De werkgroep overlegt periodiek en waarborgt dat privacy en informatiebeveiliging met een integrale blik wordt bekeken. Dit heeft als doel:

a) Een brede, structurele betrokkenheid vanuit de organisatie ten aanzien van informatiebeveiliging;
b) Het (sneller) signaleren van risico's op het gebied van informatiebeveiliging;
c) Een verbeterde afstemming, formulering en implementatie van verbeteracties en maatregelen;
d) Verschillende disciplines met elkaar in contact te brengen ten aanzien van informatiebeveiliging;
e) Het doen van voorstellen voor het prioriteren en plannen van beveiligingsmaatregelen op basis van risicoanalyse;
f) Klankbord voor de organisatie en management ten aanzien van informatiebeveiliging.

3.11 Functiescheiding

Ten aanzien van de inrichting van de organisatie geldt het beleid dat in beginsel geen enkele medewerker over de mogelijkheid beschikt om een volledige cyclus aan handelingen in een applicatie te beheren. Ten behoeve van deze 'functiescheiding' dienen rollen en verantwoordelijkheden binnen processen te zijn vastgesteld. Deze rollen zijn overeenkomstig in de relevante applicaties en systemen ingericht.
Binnen Gemeente Geertruidenberg wordt een strikte scheiding toegepast tussen IT-functies en gebruikersfuncties, tussen beheertaken en dagelijkse werkzaamheden binnen de bedrijfsprocessen.

3.12 Informatiebeveiliging in projectbeheer

Bij projecten wordt standaard een risicoanalyse uitgevoerd op basis van dit informatiebeveiligingsbeleid en geldende normen. Hiermee wordt beoogd dat informatiebeveiliging een integraal onderdeel is van de projectaanpak. In het 'programma van eisen' voor nieuwe informatiesystemen of wijzigingen/uitbreidingen van bestaande informatiesystemen moeten relevante beveiligingseisen worden opgenomen.

3.13 Controle en verantwoording

Dit strategisch beleid is een verantwoordelijkheid van het bestuur van de gemeente Geertruidenberg. De bestuurders en de clustermanagers van de gemeente zullen volgens de 10 principes (zie hoofdstuk 2.5) voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door
het geven van voorbeeldgedrag en het vragen om informatie. De clustermanagers zijn verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. De clustermanagers rapporteren daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.14 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). De ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke clustermanagers. De clustermanagers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

DigiD-aansluitingen dienen te voldoen aan de beveiligingsmaatregelen zoals gespecificeerd in het normenkader van Logius (zie Normenkader 3.0 voor ICT-beveiligingsassessments DigiD, gepubliceerd op 1 augustus 2022). Deze aansluitingen worden jaarlijks onderworpen aan een audit en zijn onderdeel van de ENSIA.

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.

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

Vastgesteld op: …….. 2025 door het college van B&W van gemeente Geertruidenberg.