Informatiebeveiligingsbeleid

2018

GEMEENTE OSS

De samenwerkende Chief Information Security Officer's (CISO's) van de gemeenten Bernheze, Landerd, Oss en Uden hebben dit document gemaakt. Wil je nog meer weten over informatiebeveiliging? Heb je andere beveiligingsvragen, ideeën of opmerkingen? Je kunt altijd contact opnemen met de CISO.

Inhoud

1. Inleiding

Voor u ligt het informatiebeveiligingsbeleid van de gemeente Oss. Deze versie is een herziening van het informatiebeveiligingsbeleid 2014. Een belangrijke gebeurtenis voor informatieveiligheid bij gemeenten is de Buitengewone Algemene Ledenvergadering van de VNG (BALV) in 2013 geweest. Daar heeft de meerderheid van de leden de Resolutie Informatieveiligheid aangenomen.

In deze resolutie is besloten dat:

1. Informatieveiligheid onderdeel wordt van collegeambities en opgenomen wordt in de portefeuille van één van de leden van het college van B&W.
2. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.
3. Gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) vaststellen als hét gemeentelijke basisnormenkader voor informatieveiligheid.
4. Gemeenten informatieveiligheidsbeleid vaststellen aan de hand van de Baseline Informatiebeveiliging Gemeenten. Uitvoering van dat beleid wordt gebaseerd op eigenstandige risicoafwegingen. Gemeenten zijn zich daarbij bewust van de (continu veranderende) informatieveiligheidsrisico’s die ze lopen en nemen hierop adequate maatregelen.
5. Gemeenten informatieveiligheid bestuurlijk en organisatorisch borgen door aansluiting in de reeds bestaande planning- en controlcyclus.
6. Gemeenten de lokale invulling rondom het thema van informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners. Gemeentelijke kwetsbaarheden, specifieke maatregelen en auditrapportages zijn niet openbaar.

De resolutie en het daaruit ontstane IBD modelbeleid uit 2014 zijn nog steeds actueel en blijven daarmee de basis voor dit herziene beleid. Dit beleid is de kapstok waaraan domein specifiek beleid (zoals BRP, SUWI en DigiD) kan worden opgehangen.

Het beleid behelst acht uitgangspunten voor informatieveiligheid. In een apart document, de bijlage bij dit beleid, wordt een en ander nader toegelicht.

2. Informatiebeveiligingsbeleid

Het bestuur en management speelt een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, 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 het informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is 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. Dit beleid bevat een bijlage met nadere aanwijzingen.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: AVG, BRP, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIG:

1. Alle informatie en informatiesystemen vallen onder dit beleidskader van informatiebeveiliging en zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)-management, met het **College van B&W als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens, privacy van burgers en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door **periodieke controle, organisatie brede 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.
3. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.

4. De **CISO** ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover zo nodig rechtstreeks aan het college.
5. De gemeente stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.
6. De gemeente kiest voor een optimale beveiliging van de haar toevertrouwde informatievoorziening en passende maatregelen. Een optimale veiligheid ontstaat door het zorgvuldig **afwegen van afhankelijkheid en kwetsbaarheid** van gemeentelijke processen en risico's versus kosten/consequenties van beveiligingsmaatregelen. Hierbij wordt een balans gezocht tussen risico's en kosten/consequenties van de benodigde beveiligingsmaatregelen.
7. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld.** Op operationeel niveau door medewerker of management. Op strategisch en tactisch niveau door directie of college. Alle medewerkers van de gemeente worden bewust gemaakt van en getraind in het gebruik van beveiligingsprocedures.
8. 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.

Dit IB-beleid treedt in werking na vaststelling door college van B&W. Hiermee komt het oude IB-beleid van de gemeente Oss van 2014 te vervallen.

Aldus vastgesteld door burgemeester en wethouders van Oss op [DATUM],

De secretaris,
[SECRETARIS]

De burgemeester,
[BURGEMEESTER]