GEMEENTE Berg en Dal

GEMEENTEBLAD

Officiële uitgave van de gemeente Berg en Dal

Nr. 152562

4 september 2017

Informatiebeveiligingsbeleid gemeente Berg en Dal

1. Inleiding

De gemeente Berg en Dal is een overheidsorganisatie waarin gewerkt wordt met vertrouwelijke informatie. Mede door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties voor gemeenten van groot belang. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening. Goede informatiebeveiliging is een vereiste om hierin te voorzien.

Onder informatiebeveiliging wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie. Deze informatiebeveiliging is nodig om een goede en veilige dienstverlening naar burgers en bedrijven te garanderen.

Bij het opstellen van het informatiebeveiligingsbeleid is met nadruk rekening gehouden met de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG). De BIG is opgesteld door de Informatiebeveiligingsdienst (IBD) in opdracht van de Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De BIG dient als norm voor informatiebeveiliging voor alle Nederlandse gemeenten. Het college van Berg en Dal heeft op 12 april 2016 ingestemd met een integrale aanpak informatiebeveiliging, privacy en melding datalekken. Onderdeel van dit besluit is het voorstel implementatie BIG in de gemeente Berg en Dal. Daarmee conformeert de gemeente zich aan de 303 normen uit de BIG. Deze vormen de basis voor het vast te stellen informatiebeveiligingsbeleid (zie ook https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/).

Informatiebeveiliging is geen zaak die alleen de ICT-afdeling aangaat. Een groot deel van beveiligingsnormen zoals ISO 27001 en de BIG gaan over beveiligingsmaatregelen die niet onder verantwoording van ICT liggen, maar op het terrein van bestuur, personeelszaken, burgerzaken, sociale zaken, facilitair en de afdelingshoofden.

Een zorgvuldige informatiebeveiliging vormt ook de basis om te kunnen voldoen aan de verschillende audits, zoals: BRP, PUN (Paspoort Uitvoeringsregeling Nederland, reisdocumenten), BAG, SUWI, DigiD.

2. Doelstelling

Het informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om informatie te beschermen en te waarborgen, waarmee de gemeente voldoet aan relevante wet en regelgeving.

Informatie is een belangrijk bedrijfsmiddel dat de gemeente op gepaste wijze beschermt. Daarom is het volgende doel gesteld ten opzichte van informatiebeveiliging:

De gemeente Berg en Dal wil ***een betrouwbare partner*** zijn voor burgers, bedrijven en ketenpartners.

Dit doel wordt bereikt door een passende set van maatregelen te treffen om risico's af te dekken en om, in het geval van incidenten, de eventuele gevolgschade (impact) van deze incidenten te beperken.

Deze maatregelen staan beschreven in het informatiebeveiligingsplan[1] (zie hoofdstuk 5).

3. Scope van het informatiebeveiligingsbeleid

3.1. Subjecten van het informatiebeveiligingsbeleid

Informatiebeveiliging en daarmee ook dit informatiebeveiligingsbeleid geldt voor alle personeelsleden in dienst van de gemeente Berg en Dal en alle externe krachten die tijdelijk of voor onbepaalde duur bij de gemeente werkzaam zijn of voor de gemeente werkzaamheden verrichten (bijv. onderaannemers, consultants, leveranciers, e.d.).

Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan de gemeente Berg en Dal eigenaar of beheerder is, dient informatiebeveiliging een onderdeel te zijn de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid van de gemeente

1) Het informatiebeveiligingsplan is het voorstel implementatie BIG dat het college op 12 april 2016 heeft vastgesteld.

Berg en Dal. Bijzondere aandacht is er voor de GR ICT Rijk van Nijmegen (iRvN) waarbij het iRvN taken voor de gemeente uitvoert.

3.2. Objecten van het informatiebeveiligingsbeleid
Het informatiebeveiligingsbeleid is van toepassing op:
- de ICT-infrastructuur (netwerk- en server hardware)
- voorzieningen voor (data)communicatie
- software
- gegevens (data)
- gegevensdragers (zoals laptops, USB-sticks maar bv. ook fysieke mappen met documenten)
- systeem- en applicatiedocumentatie
- werkplekken (zowel werkplekken op gemeentelijke locaties als thuiswerkplekken of andere externe werkplekken)
- gebouwen van de gemeente Berg en Dal (gemeentehuis, gemeentewerf, Kulturhus, sporthal, zwembad)
- het personeel.

Het informatiebeveiligingsbeleid richt dus zich niet alleen op de geautomatiseerde gegevensverwerking door middel van ICT-voorzieningen, maar uitdrukkelijk ook op de bescherming van niet geautomatiseerde gegevens (zoals fysieke documenten) en bedrijfseigendommen.

Het informatiebeveiligingsbeleid geldt voor alle informatie, hetzij mondeling, hetzij geschreven, geprint of elektronisch opgeslagen, die eigendom is van, in bewaring is bij of gebruikt wordt door welk gedeelte van de gemeente Berg en Dal dan ook. Het informatiebeveiligingsbeleid geldt ook voor alle (tijdelijke) dragers gebruikt in het creëren, verwerken, versturen, sorteren, gebruiken of controleren van gegevens en informatie.

Het informatiebeveiligingsbeleid is locatieonafhankelijk. Indien een medewerker, zakelijke relatie of leverancier of derde zich op een locatie bevindt buiten het gemeentehuis van de gemeente, maar wel met informatie of informatievoorziening (denk aan onderhoud in het veld, thuiswerken en/of webmail) van de gemeente werkt, is het beleid ook van toepassing.

3.3. Risico's
Zonder beveiligde informatie kan de gemeente Berg en Dal bloot staan aan imagoschade en financiële schade.

De risicobronnen waar de informatie en informatievoorziening aan zijn blootgesteld komen voort uit:
- de door de organisatie gewenste en gebruikte functionaliteit;
- de gebruikers van de informatiesystemen;
- de kwetsbaarheden van de ICT-infrastructuur;
- moedwillige kwaadwillende acties door eigen personeel of derden (bijvoorbeeld inbraak, ongeoorloofd gebruik, vernieling)
- externe oorzaken (natuurgeweld, maar ook technische calamiteiten zoals brand en lekkage).

De risico's zijn in kaart gebracht in een risico- en impactanalyse en maken deel uit van het informatiebeveiligingsplan (zie hoofdstuk 5).

4. Definities en belang van informatiebeveiliging
De kwaliteit van de informatievoorziening is uit te drukken in termen van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid:
- ***Beschikbaarheid*** betekent dat informatie(systemen) beschikbaar zijn op de juiste momenten. Hierdoor hebben burgers, bedrijven en organisaties toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en hun dienstverlening richting de burgers, bedrijven en organisaties ongestoord uit te kunnen voeren.

  De informatiesystemen moeten voldoen aan een beschikbaarheid tijdens kantoortijd van minimaal 95%. Buiten kantoortijd zijn er geen beschikbaarheidseisen met uitzondering van voorzieningen in het kader van rampenbestrijding. In het geval van uitval van bedrijfsprocessen en/of informatiesystemen ten gevolge van een calamiteit dient de dienstverlening binnen 48 uur hersteld te zijn.

- ***Integriteit*** betekent het waarborgen van de correctheid en de volledigheid van de informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het van belang dat de correcte informatie tijdig aanwezig is in de systemen.

- ***Vertrouwelijkheid*** betekent dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn. Voor de gemeente is het van belang dat vertrouwelijke informatie zoals de persoonsgegevens van burgers en gegevens van bedrijven alleen toegankelijk is voor bevoegden. Of een persoon bevoegd is, bepaalt de taak en verantwoordelijkheid of functieomschrijving van de betreffende persoon.

- ***Controleerbaarheid*** betekent het gemak waarmee de volledigheid en correctheid van informatie is te controleren, zelfs na een bepaalde periode. De verantwoordelijke personen en afdelingen treffen maatregelen, zodat op ieder gewenst moment en periodiek de gegevens in de informatiesystemen zijn te controleren. Deze controle kan bestaan uit een intern of extern onderzoek.

5. Informatiebeveiligingsplan
Voor het uitvoeren van het informatiebeveiligingsbeleid is een informatiebeveiligingsplan vereist. Als onderdeel van het informatiebeveiligingsplan is een GAP- en risicoanalyse uitgevoerd. Op basis van de risicoanalyse zijn maatregelen geselecteerd uit de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) .[2] Deze maatregelen moet de gemeente op basis van het risicoprofiel (de dreigingen, kwetsbaarheden en impact op de organisatie) met prioriteit implementeren[3].

Het normenkader voor de maatregelen staat benoemd in de tactische BIG. In het informatiebeveiligingsplan staat wat de maatregel inhoudt, op welke manier, door wie en wanneer de maatregel wordt ingevoerd. Het informatiebeveiligingsplan wordt één keer per jaar herijkt en vastgesteld door het MT.

De BIG is opgesteld op basis van een algemeen risicoprofiel over alle gemeenten en richt zich niet op alle voor de gemeente Berg en Dal relevante risicobronnen en de gevolgen. Het kan zijn dat een informatiesysteem of bedrijfsproces meer beveiligingsmaatregelen nodig heeft dan in de BIG staan beschreven. Bijvoorbeeld de maatregelen die specifiek voor het sociaal domein en burgerzaken vereist zijn. Om vast te stellen of voor een informatiesysteem of bedrijfsproces meer beveiligingsmaatregelen gewenst zijn, wordt een dataclassificatie uitgevoerd voor informatiesystemen en bedrijfsprocessen. Vanuit het resultaat van een dataclassificatie, worden de maatregelen vastgesteld en opgenomen in de PDCA-cyclus van informatiebeveiliging. De PDCA-cyclus wordt nader toegelicht en uitgewerkt in het informatiebeveiligingsplan.

6. Organisatie van informatiebeveiliging
De informatiebeveiligingsorganisatie beschrijft de verantwoordelijkheden, taken en bevoegdheden die met betrekking tot informatiebeveiliging per functie of rol verankerd zijn.

De inrichting van de informatiebeveiligingsorganisatie is beschreven in het document ‘informatiebeveiligingsorganisatie gemeente Berg en Dal’.

7. Wet- en regelgeving
Er zijn wettelijke eisen gesteld aan de beveiliging van gegevens en informatiesystemen. Voorbeelden hiervan zijn te vinden in:
- de ***Wet Bescherming Persoonsgegevens (Wbp)*** gaat in op de bescherming van persoonsgegevens in gestructureerde gegevensverwerkingen. De gemeente dient volgens deze wet ervoor zorg te dragen dat persoonsgegevens van burgers, bedrijven, medewerkers, leveranciers en overige belanghebbenden worden beschermd tegen onrechtmatige verwerking van of onbevoegde toegang tot deze gegevens.
- de ***Wet Computercriminaliteit II***. Deze wet gaan in op computergerelateerde strafbare handelingen. De gemeente dient door middel van adequate informatiebeveiligingsmaatregelen ervoor te zorgen dat deze wet door medewerkers van de gemeente Berg en Dal of door derden waarvoor de gemeente verantwoordelijk is niet wordt overtreden.
- ***Burgerlijk Wetboek*** , de ***Telecommunicatiewet***, de ***Auteurswet***, de ***Wet op de Jaarrekening***, de ***Archiefwet*** en het ***Wetboek van Strafvordering***, etc. Deze bevatten in het algemeen een resultaatverplichting tot een passend niveau van informatiebeveiliging.

De BIG is een afgeleide van de Code voor Informatiebeveiliging (NEN/ISO 27002). Deze code bevat elf categorieën waarop informatiebeveiliging betrekking heeft. Deze categorieën zijn:
- Beveiligingsbeleid
- Organisatie van informatiebeveiliging

2) Tactische BIG: https://www.ibdgemeenten.nl/wp-content/uploads/2015/07/15-0727-Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.01.pdf
3) Zie document ‘voorstel implementatie BIG gemeente Berg en Dal’.

- Classificatiebeheer van bedrijfsmiddelen
- Personele beveiligingseisen
- Fysieke- en omgevingsbeveiliging
- Beheer van communicatie- en bedieningsprocessen
- Toegangsbeveiliging
- Verwerving, ontwikkeling en onderhoud van informatiesystemen
- Incidentmanagement
- Bedrijfscontinuïteitsmanagement
- Naleving

De onderwerpen in de BIG zijn gebaseerd op de indeling van de NEN/ISO-normering voor informatiebeveiliging (NEN/ISO-27001 en -27002). Aangevuld met de specifieke wetgeving/regels binnen thema's als:

- BRP (Basisregistratie persoonsgegevens)
- BAG (Basisregistraties Adressen en Gebouwen)
- WOZ (Basisregistratie Waardering Onroerende Zaken)
- BGT (Basisregistratie Grootschalige Topografie)
- SUWI (wet Structuur Uitvoering Werk en Inkomen)
- Participatiewet, Wmo en Jeugdwet
- DigiD (Digitale Identiteit bij de overheid)
- PUN (Paspoort Uitvoeringsregeling Nederland)
- Wbp (Wet bescherming persoonsgegevens) waaronder de Wet meldplicht datalekken
- Archiefwet
- Wet algemene bepalingen omgevingsrecht (Wabo), Wet Ruimtelijke Ordening (WRO) etc.

Deze categorieën en regels per thema komen terug in de toegewezen rollen binnen de informatiebeveiligingsorganisatie van Berg en Dal.

8. Werking en geldigheidsduur
Het informatiebeveiligingsbeleid treedt in werking na vaststelling door het college van B en W. Het college heeft op 5 juli 2016 dit beleid vastgesteld. Na deze vaststelling komt enig voorgaand informatiebeveiligingsbeleid van de gemeente Berg en Dal te vervallen.

Daarnaast evalueert en beoordeelt de CISO het informatiebeveiligingsbeleid na 5 jaar op relevantie en actualiteit. Indien noodzakelijk stelt de CISO het document voortijdig bij en laat het vaststellen door het college van B en W.

Het informatiebeveiligingsplan (hoofdstuk 5) wordt één keer per jaar herijkt door de CISO en vastgesteld door het MT.
De informatiebeveiligingsorganisatie (hoofdstuk 6) wordt herijkt door de CISO wanneer vereist en vastgesteld door het MT.