gemeente Berkelland

GEMEENTEBLAD

Officiële uitgave van de gemeente Berkelland

Nr. 27678

6 februari

2019

Besluit van het college van burgemeester en wethouders van de gemeente Berkelland houdende regels omtrent Informatiebeveiliging vastgestelde beleidskaders 2019

1. Inleiding

In dit document is het gemeentebreed informatiebeveiligingsbeleid beschreven van de gemeente Berkelland.

Het doel van informatiebeveiliging is het:
- voorkomen van uitval van ICT systemen (beschikbaarheid en continuïteit)
- hebben en behouden van juiste, actuele en volledigheid van gegevens (ntegriteit en betrouwbaarheid van data)
- afschermen van toegang tot informatie voor onbevoegden (vertrouwelijkheid en exclusiviteit van informatie)
- achteraf kunnen vaststellen van en toezien op het gebruik van ICT systemen (controleerbaarheid).

Het informatiebeveiligingsbeleid is gebaseerd op de internationale standaarden voor informatie-beveiliging: NEN/ISO 27001 en NEN/ISO 27002. Voornamelijk op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgesteld. Deze Baseline Informatie-beveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd.

Hierbij geldt:
- Er is wetgeving waar altijd aan voldaan moet worden, zoals bijvoorbeeld de Wet Basisregistratie Personen (BRP), Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi), Basisregistraties Adressen en Gebouwen, Paspoort Uitvoeringsregeling Nederland, maar ook de archiefwet en de Wet bescherming persoonsgegevens.
- De uitgangspunten uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) zijn leidend.
- Met samenwerkingsverbanden en/of marktpartijen worden door het college gemeenschappelijke normen afgesproken. Uitgangspunt is daarbij de BIG, waarbij er ruimte is voor afweging en prioritering op basis van het ‘pas toe of leg uit’ principe.
- Het college is bestuurlijk verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid.
- De algemeen directeur/ gemeentesecretaris is verantwoordelijk voor het stellen van normen en kaders en het geven van sturing ten aanzien van de veiligheid van informatie. Hij belegt verantwoordelijkheden voor informatiebeveiligingscomponenten, –systemen en –taken bij de zelforganiserende teams en/of bij specifieke functionarissen. Hij houdt daarbij rekening met een functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken. Hij wijst een coördinator privacybescherming en informatieveiligheid en CISO aan.

De kaders zijn zodanig opgezet dat het een naslagwerk vormt voor hen die direct betrokken zijn bij de informatieveiligheid en hier in hun werk of project aandacht aan moet besteden. De intentie is niet dat alle medewerkers exact weten wat er in het gemeentebreed informatiebeveiligingsbeleid staat, maar wel weten dat er kaders zijn, hoe het te gebruiken, wat de belangrijkste uitgangspunten zijn en bij wie hulp is te vinden.

In 2016 is er voor het laatst een volledig naar de laatste inzichten opgesteld beleids- en beheerkader voor de gemeente Berkelland vastgesteld. In 2017 is deze geactualiseerd naar de eisen en aanpassingen als gevolg van de invoering AVG, het ENSIA veranwoordingsproces en organisatorische inpassing van Functionaris Gegevensbescherming, CISO en coördinator privacybescherming en informatieveiligheid.

Deze aanpassing betreft een update voor het gebruik van Suwinet. De gemeente dient zelf een security officer, gemandateerde en applicatiebeheerder van de Sociale dienst Oost Achterhoek aan te wijzen. Die taak wordt hier aan de gemeentesecretaris toegewezen.

2. Visie informatiebeveiliging gemeente Berkelland

Het belang van informatie(veiligheid)
Informatie is één van de voornaamste bedrijfsmiddelen van Berkelland. Het verlies van gegevens, uitval van ICT en/of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering. Informatieveiligheid is alleen daarom al van groot belang. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Het kan ook leiden tot imagoschade.

Informatiebeveiliging (IB) is het proces dat deze belangen dient.

Visie

Een betrouwbare[1] informatievoorziening is noodzakelijk voor het goed functioneren van de gemeentelijke organisatie en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is primair gericht op bescherming van gemeentelijke informatie. De focus is gericht op informatie(uitwisseling) in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over beschikbaarheid van informatiesystemen en afscherming van gegevens. Het gaat ook om de bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat ook niet alleen over ICT techniek: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid. Over de privacy en bescherming van persoonsgegevens worden afzonderlijk aanvullende maatregelen getroffen. De Europese Algemene Verordening Gegevensbescherming stelt per 25 mei 2018 aanvullende eisen. Hiervoor zijn in het Privacybeleid op 11 december 2018 aanvullende kaders gesteld.

Doelstelling
Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende organisatorische, procedurele en technische maatregelen om gemeentelijke informatie te beschermen en te waarborgen. De gemeente Berkelland streeft er naar om 'in control' te zijn en daarover op professionele wijze bestuurlijke verantwoording af te leggen aan ketenpartners en gemeenteraad. In control betekent in dit verband dat:

- de gemeente weet welke maatregelen genomen zijn
- er een SMART-planning is van de maatregelen die nog nodig zijn
- dit geheel via de ENSIA verantwoording verankerd is in de PDCA-cyclus.

Uitgangspunten

- Het informatiebeveiligingsbeleid van de gemeente Berkelland is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.
- Het beleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)[2] .
- Het IB-beleid wordt vastgesteld door het college van burgemeester en wethouders. De algemeen directeur/gemeentesecretaris herijkt periodiek het IB-beleid en stelt een beheerkader vast.

Risicobenadering

- De aanpak van informatiebeveiliging (IB-beleid) in de gemeente Berkelland is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG/KING (GAP-analyse) en de mate waarop in Berkelland daarvoor risico wordt gelopen.Er is een standaard pakket aan maatregelen. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de

1) Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.
2) Daarbij geldt het 'pas toe of leg uit ' principe

informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar: **risico = kans x impact**.

Doelgroepen

- Het gemeentelijk IB-beleid is van toepassing op alle in- en externe gebruikers van de gemeentelijke informatievoorziening:

Doelgroep	**Relevantie / verantwoordelijkheid voor IB-beleid**
Gemeenteraad	Controlerende taak
College van B&W	Integrale verantwoordelijkheid
Algemeen directeur/ gemeentesecretaris	In sturende zin verantwoordelijk voor kaderstelling en sturing Implementatie
Zelforganiserende teams (proceseigenaren)	Sturing op informatieveiligheid en controle op naleving
Team Opdrachtgevers	Maken van afspraken over veilig gebruik en bescherming ICT en informatievoorziening met samenwerkingsverbanden (o.a. Sociale Dienst Oost Achterhoek, Omgevingsdienst Achterhoek en Gemeentelijk Belastingkantoor Twente)
Medewerkers	Gedrag en naleving
Informatiebeheerders	Classificatie: bepalen beschermingseisen van informatie
Beleidmakers	Planvorming binnen IB-kaders
Functionaris Gegevensbescherming (FG)	Intern toezichthouder voor bescherming van persoonsgegevens en privacy
Coördinator privacybescherming en informatieveiligheid	Dagelijkse coördinatie van Informatiebeveiliging en bescherming persoonsgegevens en privacy
CISO	Intern toezichthouder voor informatieveiligheid en coördinator ENSIA
Security Officer Suwinet	het aanspreekpunt en de verantwoordelijke voor alle activiteiten, op het gebied van informatiebeveiliging rondom Suwinet en rapporteert direct aan het gemeentebestuur
Senior concern adviseur	Adviseur kwaliteit, (interim) control en interne audits
Werkgroep Privacybescherming en informatiebeveiliging	Overleg tussen FG, CISO, coördinator privacybescherming en informatieveiligheid en concern controller waar alle taken (beleid, uitvoering, auditing en toezicht) op elkaar af te stemmen.
Team Personeel	Arbeidsvoorwaardelijke zaken
Opdrachtgever Gebouwen en Kunstwerken	Fysieke toegangsbeveiliging gemeentehuis en gemeentelijke gebouwen
ICT-diensten (en -ontwikkelaars)	Technische beveiliging
Accountant en auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance

Scope

- De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en 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 gemeentelijke IB-beleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. [3]

Werking

Dit IB-beleid treedt in werking per 1 januari 2019.

3) Bijvoorbeeld SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen), DigiD en gemeentelijke basisregistraties.

Samenhang
Aan het informatiebeveiligingsbeleid van de gemeente Berkelland wordt nadere invulling gegeven door de algemeen directeur/gemeentesecretaris, de concern opdrachtgevers en de zelforganiserende teams op basis van het 'pas toe of legt principe' uit de hoofdstukken 5 tot en met 15 uit de tactische variant van de Baseline Informatiebeveiliging Gemeenten. Deze wordt verder uitgewerkt in een beveiligingsbeheerkader.

3. Kaders informatieveiligheid gemeente Berkelland

1. Alle informatie en informatiesystemen vallen onder dit beleidskader van informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging ligt bij de algemeen directeur/gemeentesecretaris, de concern opdrachtgevers en de teams. Het college van burgemeester en wethouders is bestuurlijk eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van persoonsgegevens en privacy en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving, zoals de basisregistraties, Suwinet, Paspoorten en ID-bewijzen, maar ook de archiefwet en de Wet bescherming persoonsgegevens.
3. Het bestuur kiest voor een optimale beveiliging van de haar toevertrouwde informatievoorziening en passende maatregelen. Hierbij wordt een zorgvuldige afweging gemaakt tussen afhankelijkheid en kwetsbaarheid van de processen enerzijds en de risico's versus kosten/consequenties van de beveiligingsmaatregelen anderzijds.
4. Specifieke regels en verantwoordelijkheden voor het beveiligingsbeheer dienen te worden vastgelegd en vastgesteld door de algemeen directeur/gemeentesecretaris in overleg met de werkgroep Privacybescherming en informatiebeveiliging. Alle medewerkers van de gemeente worden bewust gemaakt van en getraind in het gebruik van beveiligingsprocedures.
5. 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.
6. Informatiebeveiliging is een continu verbeterproces. De algemeen directeur/gemeentesecretaris stelt minimaal tweejaarlijks een informatiebeveiligingsplan vast, waarin de betrouwbaarheid, de beschikbaarheid en de integriteit van de informatievoorziening organisatie breed wordt benaderd en verbetermaatregelen worden gepland.
7. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging en wordt ondergebracht in de bestaande P&C cyclus.
8. De coördinator privacybescherming en informatieveiligheid ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening
9. De CISO ziet vanuit een onafhankelijke positie toe op correcte naleving, werking, effectiviteit en kwaliteit van de maatregelen die ten aanzien van de informatieveiligheid zijn getroffen. Hij ziet op de voortgang van de uitvoering van het informatiebeveiligingsplan. Hij rapporteert hierover minimaal eens per jaar (zo nodig rechtstreeks) aan het college.
10. De algemeen directeur/gemeentesecretaris stelt middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid. Hij belegt verantwoordelijkheden bij de zelforganiserende teams en zo nodig bij organisaties met gemandateerde taken.

Dit IB-beleid treedt in werking op 1 januari 2019. Hiermee komt het oude IB-beleid van de gemeente Berkelland van 1 september 2017 te vervallen.

Borculo, 29 januari 2019,
Burgemeester en wethouders van Berkelland,

de secretaris,
M.N.J. Broers

de burgemeester,
drs. J.H.A. van Oostrum.