CVDR

Officiële uitgave van Berkelland.

Nr. CVDR420873_1

6 februari 2019

Besluit van het college van burgemeester en wethouders van de gemeente Berkelland houdende regels omtrent informatiebeveiliging Informatiebeveiliging (vastgesteld beleidskaders 2016)

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 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) is leidend.
* De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid.
* De directie, de opdrachtgever bedrijfsvoering en de zelforganiserende teams stellen aanvullend een normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het ‘pas toe of leg uit’ principe.

In 2014 en 2015 is er een actueel en volledig naar de laatste inzichten opgesteld beleids- en beheerkader voor de gemeente Berkelland ontstaan.

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 men moet wel weten dat er kaders zijn, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn.

Deze verise 2016 kent voornamelijk een aanpasing van en vertaling naar de inrichting van de eerder in 2014 en 2015 vastgestelde kaders naar de uitgangspunten van het Veranderprogramma en Berkelland / Organiseren 3.0.

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 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 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 techniek: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

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 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).
* Het IB-beleid wordt vastgesteld door het college van burgemeester en wethouders. De directie 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 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
Directie	In sturende zin verantwoordelijk voor kaderstelling en sturing Implementatie
Lijnmanagement (proceseigenaren)	Sturing op informatieveiligheid en controle op naleving
Medewerkers	Gedrag en naleving
Gegevenseigenaren	Classificatie: bepalen beschermingseisen van informatie
Beleidmakers	Planvorming binnen IB-kaders

IB-functionaris	Dagelijkse coördinatie van IB
Personeelszaken	Arbeidsvoorwaardelijke zaken
Gebouwenbeheer	Fysieke toegangsbeveiliging
ICT-diensten (en -ontwikkelaars)	Technische beveiliging
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.

Werking

Dit IB-beleid treedt in werking per 1 februari 2016. Het oude algemene IB-beleid vastgesteld op 2 juli 2013 komt hiermee te vervallen met uitzondering van de door het management specifiek vastgestelde procedures voor onder andere BRP, reisdocumenten en ID-kaarten en BAG. Ook het beleid van de Sociale Dienst Oost Achterhoek rondom de Suwinet blijven gelden.

Samenhang

Aan het informatiebeveiligingsbeleid van de gemeente Berkelland wordt nadere invulling gegeven door de directie, de opdrachtgevers bedrijfsvoering en Voormekaar en de 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.

3.Kaders informatieveiligheid gemeente Berkelland

1. Alle informatie en informatiesystemen vallen onder dit beleidskader van informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging ligt bij de directie, de opdrachtgever bedrijfsvoering, de opdrachtgever Voormekaar en de teams, met het college van burgemeester en wethouders als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming en privacy van gegevens 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. De gemeente 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 beveiligingsbeleid dienen te worden vastgelegd en vastgesteld door de directie in overleg met het managementteam. 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 directie stelt minimaal tweejaarlijks een informatiebeveiligingsplan op, waarin de betrouwbaarheid, de beschikbaarheid en de integriteit van de informatievoorziening organisatiebreed wordt benaderd.
7. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging en wordt ondergebracht in de bestaande P&C cyclus.
8. De informatiebeveiligingsfunctionaris (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 zo nodig rechtstreeks aan het college.
9. De directie stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

Dit IB-beleid treedt met terugwerkende kracht in werking op 1 februari 2016. Hiermee komt het oude IB-beleid van de gemeente Berkelland van 1 januari 2015 te vervallen.

Borculo, 4 oktober 2016,
Burgemeester en wethouders van Berkelland,
de secretaris, de burgemeester,
M.N.J. Broers drs. J.H.A. van Oostrum.