gemeente Neder-Betuwe

GEMEENTEBLAD

Officiële uitgave van gemeente Neder-Betuwe.

Nr. 110892

11 augustus 2016

Strategisch Informatiebeveiligingsbeleid 2015-2017 Gemeente Neder-Betuwe

Voorwoord

Voor u ligt het informatiebeveiligingsbeleid van de gemeente Neder-Betuwe. Deze versie is een herziening van het informatiebeveiligingsbeleid en is afgestemd met het College van burgemeester en wethouders, de directie en medewerkers van gemeente Neder-Betuwe.
In het informatiebeveiligingsbeleid is rekening gehouden met:

- De Internationale standaard voor informatiebeveiliging (ISO27001).
- De Code voor Informatiebeveiliging (NEN/ISO 27002)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- Eisen voortkomende uit van toepassing zijnde wet- en regelgeving, waaronder:
  - artikel 213a van de gemeentewet
  - de ICT-beveiligingseisen en -richtlijnen voor:
    - Basisadministratie Persoonsgegevens en Reisdocumenten (BPR)
    - Basisadministratie Adressen en Gebouwen (BAG)
    - Basisregistratie personen en Waardedocumenten (Brp)
    - Paspoort Uitvoeringsregeling Nederland (PUN)
    - Archiefwet
    - Wet structuur uitvoeringsorganisatie werk en (Suwi)
    - Wet bescherming persoonsgegevens (Wbp)
    - DigiD webrichtlijnen
  - de RODIN-richtlijnen voor digitale archivering en volledige substitutie
- Eisen gesteld door derden aan de dienst – en productlevering.

Om bovenstaande uitgangspunten op een efficiënte en effectieve wijze te kunnen beheren zijn de bijbehorende normen en maatregelen geregistreerd in een 'Informatiebeveiligings-managementsysteem' (ISMS). Het ISMS is Een integraal kwaliteitssysteem voor informatiebeveiliging conform ISO 27002:2005 (Code voor Informatiebeveiliging) en vastgelegd in het 'Informatiebeveiligingshandboek gemeente Neder-Betuwe'.
Het Informatiebeveiligingshandboek is, samen met de handboeken met operationele procedures, onderdeel van het managementsysteem van de gemeente Neder-Betuwe.

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het College van B&W. Hiermee komt het oude informatiebeveiligingsbeleid van de gemeente Neder-Betuwe zoals omschreven in het 'Handboek informatiebeveiliging, gemeente Neder-Betuwe' van 31 juli 2012 te vervallen.

1. Inleiding

Dit document legt de basis voor informatiebeveiliging binnen de gemeente Neder-Betuwe en is afgeleid van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit normenkader is vastgesteld als basis voor alle gemeenten. Daar waar van dit normenkader wordt afgeweken is het principe 'pas toe of leg uit' toegepast.
Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente Neder-Betuwe en de relevante landelijke en Europese wet- en regelgeving.
De gemeente Neder-Betuwe is een informatie verwerkende organisatie en heeft op het gebied van informatiebeveiliging taken en verantwoordelijkheden die dienstbaar zijn aan een goede bedrijfsvoering. Enerzijds komt dit vanuit wetgeving en anderzijds is informatiebeveiliging een intrinsieke verantwoordelijkheid.
Gemeente Neder-Betuwe erkent dat informatiebeveiliging steeds belangrijker vanuit:

Gemeente Neder-Betuwe erkent dat informatiebeveiliging steeds belangrijker vanuit:
- Bedrijfsbeleid, missie en visie.
- De door de burger gestelde eisen en het vertrouwen van de burger in de gemeente.
- De naleving en opvolging van wet- en regelgeving.
- Maatschappelijke verantwoording.

Gemeente Neder-Betuwe wil in alle opzichten een betrouwbare partner zijn. *Samenwerken, klantgericht werken en resultaatgerichtheid* zijn de drie kerncompetenties die van de medewerkers van de gemeente worden verlangd. Een betrouwbare informatievoorziening waarbij de informatie van burgers wordt beschermd en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens is geborgd, is hier onlosmakelijk mee verbonden.
Gemeente Neder-Betuwe onderkent in zijn bedrijfsprocessen aspecten van informatiebeveiliging die om informatiemanagement vragen en die bewaakt en gecontroleerd dienen te worden. Om zo 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen.

Het bestuur en management van de gemeente spelen 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. Daar waar het bestuur een kader stellende en beslissende rol heeft ten aanzien van de maatregelen die worden getroffen.

Gemeente Neder-Betuwe zorgt dat het beleid evenals de bijbehorende documenten regelmatig worden herzien. Zodat deze, indien nodig, aangepast kunnen worden op organisatorische veranderingen en technologische ontwikkelingen. Dit om burgers, partners, bedrijven en de interne organisatie van dienst te zijn en daarbij de informatiebeveiligingsaspecten te continueren en waar mogelijk te verbeteren.

2. Uitgangspunten informatiebeveiliging gemeente Neder-Betuwe

2.1. Het belang van informatieveiligheid

Informatie is één van de voornaamste bedrijfsmiddelen van Neder-Betuwe. 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.

2.2. Visie

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!
Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

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.

2.3. Doelstelling

Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende organisatorische, procedurele en technische maatregelen om gemeentelijke informatie te beschermen en te waarborgen.
Gemeente Neder-Betuwe geeft met dit beleid een duidelijke richting aan op het gebied van informatiebeveiliging en streeft de volgende doelen na om een adequaat niveau van beveiliging conform de BIG en alle relevante wet- en regelgeving te bereiken:

- Het bereiken van informatiebeveiligingsbewustzijn bij medewerkers, management, college en inhuurkrachten van de gemeente.
- Het inbedden van het component informatiebeveiliging in de werkzaamheden van alle organisatieonderdelen.
- Het 'in control' zijn op alle informatiebeveiligingsmaatregelen die genomen zijn en die nog nodig zijn, verankerd in een PDCA-cyclus.

Beheersing van informatiebeveiligingsaspecten wordt bereikt door een stelsel van organisatorische en technische maatregelen. Gemeente Neder-Betuwe heeft als streven om al die maatregelen te treffen die noodzakelijk zijn en die binnen alle en redelijkheid en billijkheid voor de gemeente in economische zin haalbaar zijn. Dit om de veiligheid van de informatie en het personeel te waarborgen, aan de relevante wet- en regelgeving te voldoen, de continuïteit van de bedrijfsvoering te waarborgen en om de reputatie als betrouwbare partner te beschermen.

2.4. Uitgangspunten

De uitgangspunten van het IB-beleid zijn:

- Het informatiebeveiligingsbeleid van de gemeente Neder-Betuwe 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.

2.5. Risicobenadering

De aanpak van informatiebeveiliging (IB-beleid) in de gemeente Neder-Betuwe is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)[1] van VNG/KING (GAP-analyse). Indien een systeem privacy of security gevoelig is kan het zijn dat er aanvullende maatregelen nodig zijn. Voorbeelden zijn de systemen rond de basisregistraties personen en systemen rondom de 3 decentralisaties waarvoor vanuit de wet specifieke/aanvullende maatregelen vereist worden. In dat geval 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

2.6. Doelgroepen

Het gemeentelijk IB-beleid is bedoeld voor alle in- en externe medewerkers van de gemeente:

Doelgroep	**Relevantie / verantwoordelijkheid voor IB-beleid**
Leden gemeenteraad en raadscommissies	Controlerende taak t.a.v informatieveiligheid
College van B&W	Integrale verantwoordelijkheid
Directie	Kaderstelling en 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/CISO	Dagelijkse coördinatie van IB
Personeelszaken	Arbeidsvoorwaardelijke zaken
Gebouwenbeheer	Fysieke toegangsbeveiliging
ICT-diensten (en -ontwikkelaars)	Technische beveiliging
Auditors	Onafhankelijke toetsing
Leveranciers en ketenpartners	Compliance

2.7. De reikwijdte

De reikwijdte van dit IB-beleid is dat:

- Dit beleid van toepassing is op 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 een algemene basis is. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Bijvoorbeeld voor de uitgifte van Paspoorten en Nederlandse Identiteit Kaarten, of gebruik van de Gezamenlijke elektronische Voorzieningen Suwi Service (Suwinet)voor het Sociale Domein.

2.8. Werking

Dit IB-beleid treedt in werking op de datum dat het is vastgesteld door het college van B&W. Hiermee komt het oude Informatie beveiligingsbeleid van de gemeente Neder-Betuwe, dat is vastgesteld door het college in juli 2012, te vervallen met uitzondering van de bestaande gemeentelijke procedures voor BRP, reisdocumenten en ID-kaarten en BAG. Het beleid van Beursplein Rivierenland rondom de Suwinet blijft eveneens gelden.

2.9. Samenhang

Aan het informatiebeveiligingsbeleid van de gemeente Neder-Betuwe wordt nadere invulling gegeven door de directie en het managementteam op basis van het 'pas toe of legt principe'. In het handboek informatiebeveiliging worden hiervoor beleidsregels opgenomen op alle aspecten van informatiebeveiliging uit de BIG. Het gaat hier om de volgende beveiligingsaspecten :
Organisatie van de informatiebeveiliging

- Beheer van bedrijfsmiddelen V
- Beveiliging van personeel
- Fysieke beveiliging en beveiliging van de omgeving V

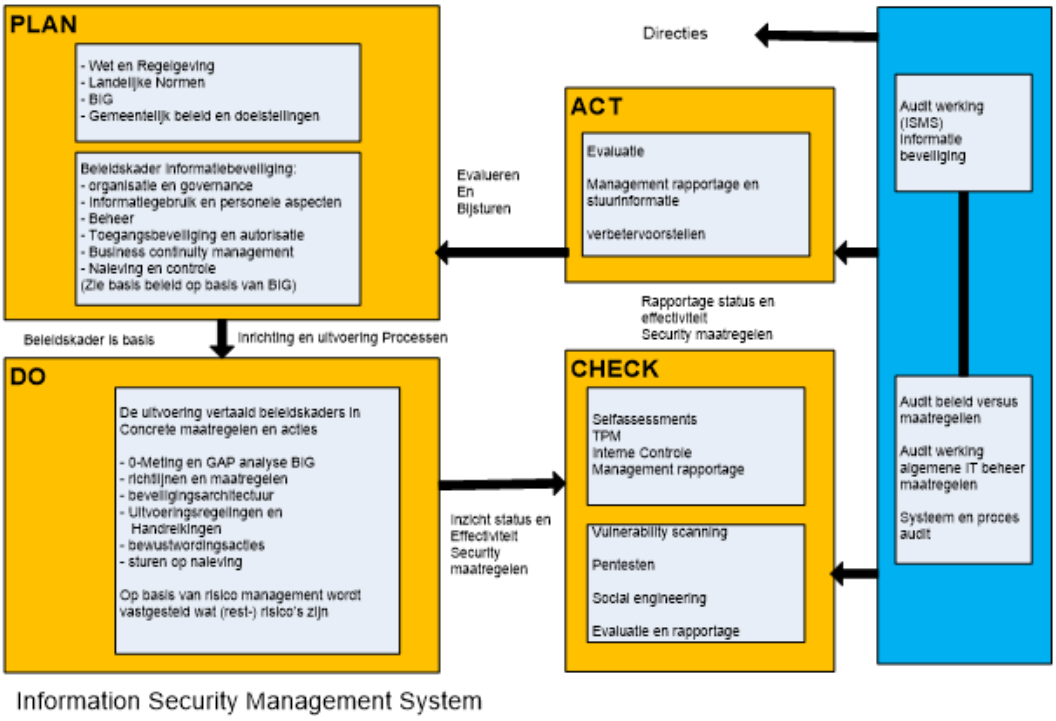
- Beveiliging van apparatuur en informatie
- Logische toegangsbeveiliging V
- Beveiligingsincidenten
- Bedrijfscontinuïteit
- Naleving

In hoofdstuk 4 “Aanpak van informatiebeveiliging “ van dit beleidsdocument wordt de aanpak van bovenstaande beveiligingsaspecten beschreven zoals die door gemeente Neder-Betuwe wordt gehanteerd.
[1] De baseline is een instrument waarmee gemeenten in staat zijn om te meten of de organisatie ‘in control’ is op het gebied van informatiebeveiliging.

3. Informatiebeveiliging managen

3.1. Beheersen maatregelen

Voor de beheersing van informatiebeveiliging aspecten hanteert gemeente Neder-Betuwe een Information Security Management System (ISMS). Het ISMS is gebaseerd op de internationale standaarden voor informatiebeveiligingsmanagementsystemen zoals opgesteld in de ISO 27001 door de International Standards Organization (ISO) die de basis vormt voor de BIG. Het ISMS bevat een informatiebeveiligingsmanagementproces dat is ingericht op basis van de ‘Deming Circle’ (Plan – Do – Check – Act).



Figuur 1 ISMS informatiebeveiliging

Concreet betekent bovenstaande dat in Neder-Betuwe:

- Vanuit de directie jaarlijks een plan wordt opgesteld voor het verbeteren van de informatiebeveiliging. Dit plan wordt vastgelegd in het handboek informatiebeveiliging.
- Het MT maatregelen treft om de beveiligingsrisico’s te verminderen en compliant te zijn aan wetregelgeving, landelijke normen en de baseline informatiebeveiliging gemeenten.
- De informatiebeveiligingsmedewerker(s) jaarlijks vaststelt welke (rest-) risico’s er zijn door middel van een risicoanalyse.
- Het MT periodiek zelfonderzoeken en interne/externe audits laat uitvoeren voor de BRP, reisdocumenten en ID-kaarten, de BAG en Suwi.
- De directie jaarlijks het informatiebeveiligingsbeleid en het handboek informatiebeveiliging evalueert en een verbeterplan laat opstellen.

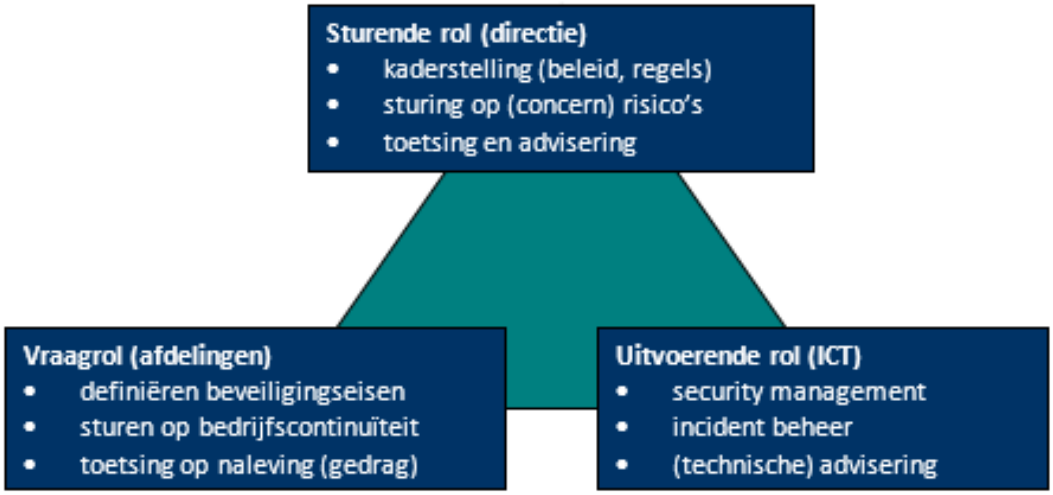
3.2. Inrichten organisatie

Door het inrichten van een informatiebeveiligingsorganisatie zorgt de gemeente Neder-Betuwe voor passende aandacht en sturing. Het College van B&W is integraal eindverantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Zij is verantwoordelijk voor de werking van het informatiebeveiligingsmanagementsysteem en zal via delegatie naar medewerkers de taken en

verantwoordelijkheden beleggen voor de implementatie en beheer van maatregelen die voortkomen uit dit beleid. Specifieke rollen die het college hierbij aanwijst zijn:

- De Chief Information Officer (CIO) is de portefeuillehouder informatiebeveiliging en is een rol op strategisch niveau binnen de gemeentelijke organisatie.
- De organisatie van informatiebeveiliging wordt namens de directie aangestuurd door de medewerker informatiebeveiliging. Tactische/operationele taken zullen gedelegeerd worden naar informatiebeveiligings functionarissen binnen de afdelingen en processen.

De directie is verantwoordelijk voor kaderstelling en sturing. De directie stuurt op concern risico's, controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden en evalueert periodiek beleidskaders en stelt deze waar nodig bij.



De afdelingen binnen de gemeente zijn verantwoordelijk voor de integrale beveiliging van hun eigen organisatieonderdelen. Iedere afdeling:

- stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie);
- is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

Alle medewerkers van Gemeente Neder-Betuwe hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen die voortvloeien uit dit beleid.
Identificatie van incidenten of het niet voldoen aan het gestelde in dit beleid dienen gemeld te worden aan de lijnmanagers of de medewerker informatiebeveiliging.
Dit beleid maakt integraal deel uit van de arbeidsvoorwaarden van Gemeente Neder-Betuwe.

3.3. Beoordeling en corrigerende maatregelen
Gemeente Neder-Betuwe zal de maatregelen die voortkomen uit dit beleid periodiek controleren middels controles vanuit AOIC en interne assessments en externe audits ten aanzien van (kosten)effectiviteit en informatieveiligheid.
Jaarlijks zal de directie het informatiebeveiligingsmanagementproces beoordelen op basis van verzamelde gegevens en informatie. Input voor deze beoordeling is o.a.:

- Registratie van incidenten en non-compliance issues.
- Registraties van controle, interne en externe audits.
- Leveranciersbeoordelingen.
- Risicoanalyse[2] output.
- Medewerkerscompetenties.
- Bewustwording sessies en -training.
- Wet- & regelgeving.

Op basis van de beoordelingen zullen waar mogelijk corrigerende en of preventieve maatregelen worden doorgevoerd. Maatregelen worden geselecteerd met het doel dat de kans op herhaling geminimaliseerd wordt. Of waardoor de doeltreffendheid van het informatiebeveiligingsmanagementsysteem wordt verbeterd en het geleverde product of dienst beter aansluit op de eisen van de burger, bedrijven en partners.

3.4. Bescherming van informatie, classificatie
Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Het doel is: waarborgen van de continuïteit, integriteit en vertrouwelijkheid van informatie en de informatievoorziening en het beperken van de gevolgen van eventuele beveiligingsincidenten.
Voor een effectieve bescherming van de informatie is vereist dat de waarde van de informatie voor de interne organisatie bekend is. Classificatie van informatie, in termen van vereiste vertrouwelijkheid, integriteit en beschikbaarheid:

- informeert het College van B&W, directie, lijnmanagers en medewerkers over wat moet worden beschermd en hoe informatiemiddelen op een standaard manier kunnen worden beschermd;
- toont de waarde van middelen aan medewerkers, zodat het bewustzijn van beveiliging binnen hun dagelijkse werkzaamheden wordt gestimuleerd;
- stelt de gemeente in staat te voldoen aan eventuele wettelijke en contractuele verplichtingen.

Classificatie van gegevens moet voldoen aan de VIR/VIRBI.
De eigenaar van de informatie blijft verantwoordelijk voor het up-to-date houden van de identificatie van informatiemiddelen en de toegekende waarde voor elk van de geïdentificeerde middelen.
Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

- **Beschikbaarheid**: hoeveel en wanneer data toegankelijk is en gebruikt kan worden. De onderscheiden niveaus zijn: niet nodig; noodzakelijk; belangrijk en essentieel.

- **Integriteit**: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). De onderscheiden niveaus zijn: niet zeker; beschermd; hoog en absoluut.

- **Vertrouwelijkheid**: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. De onderscheiden niveaus zijn: openbaar; bedrijfsvertrouwelijk, vertrouwelijk en geheim.

Met de invoering van de Baseline Informatiebeveiliging voor Gemeenten is het basis beveiligingsniveau bepaald dat geldt voor de gehele bedrijfsvoering van een gemeente. Hierdoor moeten alleen processen en systemen onderzocht worden waarvan verwacht wordt dat deze meer beveiligingsmaatregelen nodig hebben dan de Baseline. Met een classificatiemethode kan bepaald worden of het proces of systeem binnen of buiten baseline valt. Indien de classificatie hoger dan vertrouwelijk is, dan zijn extra maatregelen nodig.

Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau ‘geen’. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven. Tussen haakjes staan voorbeelden. Deze niveaus zijn bedacht om het proces van classificeren te vereenvoudigen.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers	**Hoog** het bedrijfsproces staat zeer weinig fouten toe	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*

	(bv: persoonsgegevens, financiële gegevens	*(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: gemeentelijke informatie op de website)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

Hoe geven we concreet uitvoering aan het classificeren van data en beschermingsniveaus?

Classificatie vindt plaats door de kritieke processen van de gemeentelijke organisatie te inventariseren aan de hand van: verstoring of uitval van het proces, systeem, eigenaar, gegevens, hardware. Hierbij wordt een link gelegd met de toegepaste informatiemiddelen en informatiesystemen per proces. Een voorbeeld is het proces van aanvragen in de sociale pijler.

(p4) Verstrekken producten & diensten (Sociale Pijler)	Vergunningen en ontheffingen, subsidies, verzoeken, aangiften, publieke producten, inkomens- en maatschappelijke ondersteuning	(Aan)vraag inwoner/bedrijf wonen, werken, welzijn en zorg	Besluit / beschikking/ product uit zorgsysteem	B: Essentieel	I: Hoog	V: Geheim

[2] Een risicoanalyse bestaat uit/omvat: 1. Risicogebied vaststellen (context) door het vaststellen van kritieke processen en bedrijfsmiddelen. 2. Risico assessment en evaluatie door middel van een business impact analyse en dreigingen -analyse.
Deze analyse wordt jaarlijks opgesteld/geactualiseerd vanuit het beveiligingsplan GBA en Waardedocumenten. Met de invoering van de BIG wordt deze analyse verbreed naar de organisatie en vanuit het informatiebeveiligingsbeleid opgesteld door de medewerker informatiebeveiliging.

4. Aanpak van informatiebeveiliging

4.1. Risicomanagement

Risicobewustzijn van alle medewerkers van Gemeente Neder-Betuwe is de sleutel tot een effectieve informatiebeveiliging. Risicobewustzijn wordt volledig ondersteund door de directie van Gemeente Neder-Betuwe en zal gestimuleerd worden door middel van bewustwordingssessies en publicaties via onder meer het intranet. Het risicobewustzijn wordt ook ondersteund door het opstellen en naleven van gedragscodes en gebruikersovereenkomsten en zal aandacht krijgen in functiebeschrijvingen en arbeidscontracten of op de algemene inkoopvoorwaarden gebaseerde overeenkomsten met derden.

Via de Baselinetoets en Risicoanalyse conform de opzet van de Informatie Beveiligings Dienst, worden mogelijke dreigingen en informatiebeveiligingsrisico's geïdentificeerd en geïndexeerd. De directie zal de resultaten die hier uit voortkomen beoordelen en voor 'rendabele' maatregelen een implementatieplan opstellen ter vermindering van het risico tot een acceptabel niveau.

4.2. Organisatie van de informatiebeveiliging

De organisatie van de informatiebeveiliging is beschreven in paragraaf 3.3 van dit beleidsdocument.

4.3. Beheer van bedrijfsmiddelen

IT middelen die aan medewerkers van gemeente Neder-Betuwe beschikbaar worden gesteld, dienen voor zakelijke doeleinden toegepast te worden. Opgeslagen en verwerkte informatie van of voor gemeente Neder-Betuwe op systemen van de gemeente blijft te allen tijde eigendom van gemeente Neder-Betuwe. De internationale en lokale privacy wetgeving zal gehandhaafd worden wanneer een beroep wordt gedaan op eigendomsrechten.

4.4. Beveiliging van personeel

Bij het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers wordt bewerkstelligd dat zij hun verantwoordelijkheden begrijpen ten aanzien van informatieveiligheid. Deze verantwoordelijkheden zijn vóór het dienstverband vastgelegd in een passende functiebeschrijvingen/opdracht en in de arbeidsvoorwaarden/inhuurovereenkomst. Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een ICT-protocol met betrekking tot hun beveiligingsrollen en –verantwoordelijkheden.

4.5. Fysieke beveiliging ICT-voorzieningen

Gemeente Neder-Betuwe heeft IT-voorzieningen geïmplementeerd voor de eigen bedrijfsonderdelen en locaties die onderlinge interne communicatie en samenwerking met partners, burgers en medewerkers op afstand mogelijk maakt. Deze IT-voorzieningen zijn deels in beheer en eigendom van gemeente Neder-Betuwe en deels uitbesteed. Voor de beveiliging hiervan moet door de leverancier jaarlijks een verklaring worden overlegd waarin zijn aantonen dat zijn voldoen aan alle hoogste informatiebeveili-

gingseisen. Ook aan de verbinding naar de Cloud worden hoge eisen gesteld die getoetst moeten worden. ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, dienen fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze zijn fysiek beschermd tegen toegang door onbevoegden, schade en storingen.
Voor bepaalde diensten wordt gebruik gemaakt van externe publieke netwerken zoals het internet. Hiervoor zijn er diverse beveiligingsmaatregelen en beheersmaatregelen geïmplementeerd om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen.

4.6. Beveiliging van apparatuur en informatie
Organisatorisch is het zo geregeld dat er een scheiding is van beheertaken en overige gebruikerstaken. In beginsel heeft niemand autorisaties om een gehele cyclus van handelingen in een informatiesysteem te beheersen. Bijvoorbeeld degene die inkoopt, bestelt en de opdracht verleent mag niet degene zijn die ook de betaling verricht. Of degene die werk uitvoert voor de gemeente is niet degen die het salaris uitkeert of de factuur voor inhuur betaalt. In geval van overlap hierin zoals bij de salarisadministrateur geldt het vier ogen principe. Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de proceseigenaar.

Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten. Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

Beveiligingsmaatregelen die worden getroffen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Hierbij gaat het erom dat de gemeente dit af kan dwingen als de situatie hier om vraagt. Richtlijn is dat privé apparatuur niet verbonden mag worden met het gemeentenetwerk en wel met het publieke netwerk.
ICT maakt reservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd. De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering. Dit wordt verzorgd door systeembeheer. Zij weet wat te doen/mee te nemen in de reservekopie op basis van wat de systeemeigenaren hebben aangegeven als essentiële systemen en data/gegevens. Op basis daarvan is een back-up schema opgesteld en ingericht. Jaarlijks wordt door middel van een back-up en restore test getoetst of alle essentiële programmatuur en gegevenssets zijn te herstellen.

Voor het gebruik van gemeentelijke informatie gelden de rechten en plichten zoals vastgelegd in de diverse documenten, zoals het CAR-UWO, geheimhoudingsverklaring, huisregels. De gemeente Neder-Betuwe onderschrijft daarbij artikel 2:5 (2.1.5) uit de Awb.

In de Awb staat de geheimhouding geregeld in art 2:5 (2.1.5)
Een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die gegeven, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit.

Voor de omgang met vertrouwelijke en/of geheime informatie hanteert gemeente Neder-Betuwe :

- Openbaarheid van bestuur is de regel.
- Vertrouwelijkheid kan maar dan zo kort mogelijk; en heeft geen juridische status.
- Geheimhouding is de uitzondering, maar mag alleen worden opgelegd als dat volstrekt noodzakelijk is (WOB) en daarbij moeten procedures correct worden doorlopen.

Digitale documenten van de gemeente waar burgers en bedrijven rechten aan kunnen ontlenen, maken gebruik van PKI Overheid certificaten voor tekenen en/of encryptie. Hiervoor wordt een richtlijn PKI en certificaten opgesteld. De gemeente gebruikt bijvoorbeeld een PKI certificaat ter jaarlijkse ondertekening van het "Beeld van de uitvoering" voor het Ministerie van SZW tbv de gemeenten Neder-Betuwe.
Om veilig de digitale formulieren van de Inspectie SZW te kunnen gebruiken is er op de achtergrond een certificaat geplaatst dat er voor zorgt dat de gegevens die u daar invult beveiligd worden verzonden aan de Inspectie SZW. Om die veiligheid optimaal te garanderen is, conform de voorschriften van de overheid, het nieuwste type certificaat geïnstalleerd.

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen.

4.7. Logische toegangsbeveiliging

Toegang tot informatie en IT-faciliteiten zal op basis van 'need to know' worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie.
Toegang tot informatiesystemen wordt geïnitieerd door de lijnmanager van de medewerker op basis van het toekennen van een autorisatiesprofiel welke hoort bij de medewerkersrol. Na het accorderen door de informatie- of informatiesysteemeigenaar zullen de autorisaties worden toegekend. Het ontzeggen van toegang tot informatiesystemen wordt eveneens geïnitieerd door de lijnmanager.
Na het afmelden van medewerkers die uit dienst zijn of inhuurkrachten waarvan de opdracht is gestopt worden door de informatie- of informatiesysteemeigenaar de autorisaties ingetrokken.
De functioneel beheerders van informatiesystemen zoals het Zaak-, Financieel- en HRM-systeem krijgen via P&O een toekenning op een verzoek tot toegang tot een autorisatieprofiel door. Op basis van deze toekenning verwerkt elke functioneel beheerder de autorisatie in zijn/haar systeem. Sommige informatiesystemen werken op basis van singel-sign-on via dezelfde gebruikersnaam en wachtwoord om op het netwerk in te loggen. Andere informatiesystemen zoals het HRM-systeem genereren een gebruikersnaam en de gebruiker moet zelf een wachtwoord kiezen.

4.8. Data- beveiligingsincidenten

De medewerker dient geconstateerde of vermoede data-/beveiligingslekken en beveiligingsincidenten direct te melden bij de functionaris informatiebeveiliging van de gemeente.
Beveiligingsincidenten die worden gemeld bij de ICT helpdesk, worden als zodanig geregistreerd en voorgelegd aan de security functionaris binnen ICT. Voor afhandeling geldt de reguliere rapportage en escalatielijn.
Voorbeelden van data-/beveiligingslekken en beveiligingsincidenten zullen via voorlichting en communicatie in het kader van de bewustwording duidelijk gemaakt moeten worden.
Een beveiligingslek is een zwakke plek in het systeem (hard- of software), die functies toelaat die niet toegestaan zijn, of onbevoegden toegang tot gegevens of functies verschaft. Beveiligingslekken kunnen berusten op programmeerfouten, ontwerpfouten of verkeerde configuraties. Hierbij heeft ICT een rol maar ook de applicatiebeheerders die de toegang tot systemen/data autoriseren en kunnen monitoren. Bijvoorbeeld een data-/beveiligingslek wordt vaak als eerste door ICT geconstateerd. Dit kan zijn infectie door virus, zoek zijn van gegevensdragers, etc.

4.9. Bedrijfscontinuïteit

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen.
Er worden minimaal jaarlijks oefeningen of testen gehouden om de continuïteitsplannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

4.10. Naleving

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:

- de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
- efficiency en effectiviteit van de geïmplementeerde maatregelen;
- de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.

5. Kwaliteitsbewaking

5.1. Communicatie

In de communicatie van dit beleid staat de bewustwording van de medewerkers (en ingehuurde derden) centraal en de naleving van de regels en richtlijnen. Om dit te bewerkstelligen zullen er gedragsregels opgesteld en gecommuniceerd worden zodat medewerkers weten wat er van hun verwacht wordt,

welke risico´s er zijn en welke rechten en plichten ze hebben. Veranderingen en aanpassingen in het informatiebeveiligingsmanagementsysteem worden door het management beoordeeld en intern gecommuniceerd, indien nodig ook naar relevante externe partijen.

Het college/de directie bevordert naleving en bewustwording informatiebeveiliging en bepaalt:

- wat gecommuniceerd wordt;
- wanneer gecommuniceerd wordt;
- met wie gecommuniceerd wordt;
- wie de communicatie uitvoert en;
- welke processen door de communicatie beïnvloed worden.

Dit vertaalt zich in beveiligingsrichtlijnen en aandacht voor dit thema in de interne nieuwsvoorziening. Afspraken worden vastgelegd. Naast bespreking in bijeenkomsten zijn het zaaksysteem Decos-Join en het intranet de voornaamste bronnen van informatie.

5.2. Borging

Borging vindt plaats door middel van vastlegging van de overeengekomen werkwijze. Dit kan via een of meer van de volgende vormen van vastlegging: procesbeschrijvingen, richtlijnen, gedragscode, procedures, werkinstructies of tooling. Wat er ook wordt vastgelegd deze informatie dient voor alle medewerkers toegankelijk te zijn en zal via het intranet verspreid worden, zodat in het geval van incidenten en calamiteiten deze snel en eenduidig toegankelijk is.
Het gaat hier voor een groot deel om zaken die al bestaan maar die nog niet gebundeld zijn en die geactualiseerd moeten worden. Hierbij zijn betrokken de beveiligingsfunctionaris BRP en waarde documenten, de P&O adviseur, ICT coördinator en de informatiebeveiligingsfunctionaris.

5.3. Geldigheid en evaluatie

Het College van B&W van gemeente Neder-Betuwe is eigenaar van dit beleidsdocument. Het beheer, opstellen en actueel houden van het beleidsdocument is de verantwoordelijkheid van de namens de directie.
Dit beleid is drie jaar geldig en wordt minimaal één keer per jaar geëvalueerd samen met het handboek informatiebeveiliging, dit met het oog op:

- De toereikende en de tactische en operationele uitvoering ervan.
- De stand van de techniek (beveiliging en bedreiging).
- Voortschrijdend inzicht.
- Veranderende wet- en regelgeving of organisatie.

Op grond van de jaarlijkse beoordeling, veranderende wet- en regelgeving of door andere omstandigheden, kan dit beleid tussentijds bijgesteld worden.

5.4. Naleving

Naleving van het beleid wordt gecontroleerd. Niet naleven van het beleid kan disciplinaire maatregelen tot gevolg hebben, conform lokale regel- en wetgeving. Jaarlijks zijn er diverse audits, zelfevaluaties, bewustwordingssessies, mistery guest en de risicoanalyse, deze acties zorgen ervoor dat het beleid wordt gecontroleerd op zijn toepasbaarheid, volledigheid en werking.

6. Informatiebeveiligingsbeleid gemeente Neder-Betuwe

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. Het bestuur krijgt de inschatting van het belang en de risico's voorgelegd vanuit de organisatie en bepaalt de kaders en maakt de afwegingen rondom de maatregelen voor informatieveiligheid. 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 zij 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 strategische beleid is nader uitgewerkt op tactisch niveau met nadere concrete aanwijzingen.in het handboek informatiebeveiliging.

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: CBP, GBA, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).[3]
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

Dit IB-beleid treedt in werking na vaststelling door het College van B&W. Hiermee komt het oude informatiebeveiligingsbeleid van de gemeente Neder-Betuwe zoals omschreven in het *Informatiebeveiliging Handboek* van juli 2012 te vervallen.

Bij het vaststellen van het informatiebeveiligingsbeleid worden de volgende besluiten genomen:

- In te stemmen met het Informatiebeleid gemeente Neder-Betuwe met ingang van datum besluit.
- In het jaarverslag een vast onderdeel 'informatiebeveiliging' op te nemen.
- In te stemmen met de uitvoering van dit beleid.
- In te stemmen met de uitwerking van dit beleid in het handboek informatiebeveiliging.
- In te stemmen met de kwaliteitsbewakingsvoorstellen voor communicatie, borging van de PDC-cylcus via het Information Security Management System (ISMS) , jaarlijkse evaluatie en controle op naleving.
- Jaarlijks het informatiebeveiligingsbeleid en en het ISMS te beoordelen op basis van een evaluatierapport en een rapportage uit het ISMS met incidenten en restrisico's.

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. De verantwoordelijkheid voor informatiebeveiliging ligt bij het management, met het College van B&W 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. Een optimale veiligheid ontstaat door het zorgvuldig afwegen van afhankelijkheid en kwetsbaarheid van gemeente processen en risico's versus kosten/consequenties van beveiligingsmaatregelen. Hierbij wordt een balans gezocht tussen risico's en kosten/consequenties van de benodigde beveiligingsmaatregelen.

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/ 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. In tegenstelling tot het beleid stelt de gemeente minimaal tweejaarlijks een informatiebeveiligingsplan op, waarin de betrouwbaarheid, de beschikbaarheid en de integriteit van de informatievoorziening organisatie breed wordt benaderd.

7. 'Plan, Do, Check en Act' vormen samen het managementsysteem van informatiebeveiliging en wordt ondergebracht in de bestaande P&C cyclus.

8. De medewerker informatiebeveiliging 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 gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

[3] De baseline is een instrument waarmee gemeenten in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging.
Aldus vastgesteld door het College van B&W van gemeente Neder-Betuwe op de datum:

J.J.J. van Huffelen MPG BBA,
de secretaris
Ir. C.W. Veerhoek
de burgemeester