INFORMATIE
BEVEILIGINGS
DIENST

CONTRACTMANAGEMENT

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Contractmanagement

Versienummer
1.02

Versiedatum
Augustus 2016

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

versie	datum	Opmerkingen
1	08-04-2014	Initiële versie
1.02	19-08-2016	Kleine tekstuele aanpassingen, links aangepast, verwijzingen naar andere BIG documenten aangepast of toegevoegd.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers.

De IBD heeft de volgende doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van een dergelijk project.
4. het faciliteren van kennisdeling tussen gemeenten op het vlak van informatiebeveiliging

Hoe realiseert de IBD haar doelen?

Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is er één van.
Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij gelden de volgende uitgangspunten:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, Wbp, 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 in de naleving van dat kader voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Het doel van dit document is aanwijzingen te geven omtrent contractmanagement en beveiligingseisen.

Doelgroep
Dit document is van belang voor het management van de gemeente, inkopers, contractmanagers en de ICT-afdeling.

Relatie met overige producten
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging voor Gemeenten
- Informatiebeveiligingsbeleid van de gemeente
- De bewerkersovereenkomst
- De Service Level Agreement (SLA)
- Toegangsbeheer
- Verklaring omtrent gedrag (VoG)
- Geheimhouding
- Inkoopvoorwaarden

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
6.2.1 ‘Identificatie van risico's die betrekking hebben op externe partijen’.
6.2.3 ‘Beveiliging behandelen in overeenkomsten met een derde partij’.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoud

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) beschrijft maatregelen die te maken hebben met identificatie van risico's en benoemt hierbij onder andere informatiebeveiligingsmaatregelen die te maken hebben met externe partijen en overeenkomsten. Een voorbeeld hiervan is de bewerkersovereenkomst die nodig is bij het bewerken van persoonsgegevens door een derde partij.
Binnen gemeenten worden contracten met externe partijen beheerd die al of niet een informatieveiligheidscomponent kunnen hebben. Daarmee heeft de contractmanager, of iemand met een vergelijkbare rol binnen de gemeente te maken met beveiligingsmaatregelen in de contracten.

1.1 Doelstelling contractmanagement

Contractmanagement is het proces dat er onder andere voor zorgt dat contracten beheerd worden. De taken die de contractbeheerder uitvoert zijn onder andere:

- Opstellen, aangaan en nakomen van contracten.
- Sturen van de leveranciersrelatie.
- Bewaken en vergroten van kwaliteit van de dienstverlening die aan de gemeente geleverd wordt.
- Voeren van contractonderhandelingen
- Handhaven van de overeengekomen contractsbepalingen

Informatieveiligheid is in dit verband ook een kwaliteitsaspect dat de contractmanager dient te bewaken.

1.2 Indeling van dit document:

Hoofdstuk 1: Inleiding over contractmanagement.
Hoofdstuk 2 : Contractmanagement en -beveiliging.
Bijlage: Aanvullend contractmanagement beleid voor de gemeente.

1.3 Aanwijzing voor gebruik

Deze handleiding is geschreven om informatiebeveiligingsmaatregelen die te maken hebben met contractmanagement uit te werken. Het doel is dat contractmanagers of diegene die van gemeentewege te maken krijgt met contracten met derden weet welke informatiebeveiligingsaspecten/omgang met gevoelige gegevens een rol spelen bij het uitvoeren van het contractmanagementproces. Dit document gaat slechts over deze aspecten van het contractmanagement- of inkoopproces binnen een gemeente.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

2 Contractmanagement en -beveiliging

2.1 Algemeen

In 2013 hebben de gemeenten de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) omarmd. De beveiligingseisen uit deze BIG hebben ook aandacht voor contracten met derden. Daarmee heeft de gemeente een normenkader in handen om beveiligingseisen en -wensen die nodig zijn in contracten met derden uit te werken. De IBD heeft al een aantal producten opgeleverd die een relatie hebben met beveiligingseisen in contracten. Deze zijn:

- Een voorbeeld SLA
- Een model voor een bewerkersovereenkomst
- Een aanwijzing voor beveiligingseisen in algemene inkoop voorwaarden.

Dit document gaat uit van de rol contractmanager, niet iedere gemeente heeft hiervoor een aparte functionaris in dienst. Echter, vergelijkbare taken kunnen ook door een andere functionaris worden uitgevoerd. De contracten kunnen ook worden beheerd binnen de ICT-afdeling, door een financiële afdeling of bijvoorbeeld door een afdelingshoofd.

2.2 Wat te doen vooraf aan een aanbesteding of inkoopproces?

Voorafgaand aan een aanbesteding moeten veiligheidsrisico's worden onderkend die op een product of dienst inwerken. Daarmee wordt de basis gelegd voor beveiligingseisen en -wensen die op een bepaalde plaats in de contractdocumenten weer aan bod moeten komen. Hierover moeten afspraken worden vastgelegd in de overeenkomst/het contract. Een voorbeeld daarvan is dat vooraf vastgesteld wordt of er (bijzondere/gevoelige)persoonsgegevens, waar de gemeente zeggenschap over heeft, in systemen bij een derde partij terecht kunnen komen. Een van de maatregelen die dan moet worden genomen, is het afsluiten van een bewerkersovereenkomst. In deze bewerkersovereenkomst zitten alle eisen (zoals het versleutelen van de gegevens) en wensen opgenomen die te maken hebben met de integriteit en exclusiviteit van die gemeentelijke (bijzondere/gevoelige) persoonsgegevens. Een ander voorbeeld is dat een systeem wordt gebruikt waar de gemeente bepaalde beschikbaarheidseisen heeft die in het contract en de SLA terecht komen.

Waar moet men voorafgaand aan een aanbesteding aan denken:

- Is er binnen de gemeente een stappenplan/beleid om te borgen dat de juiste beveiligingsmaatregelen benoemd worden in het contract met derden.
- Om vast te stellen wat de juiste beveiligingsmaatregelen zijn voert men binnen de gemeente de volgende activiteiten uit:
    - een verkorte risicoanalyse of baseline toets;
    - eventueel een Privacy Impact Assessment (PIA);
    - Een volledige risicoanalyse.
- Is er een formeel proces waar bijvoorbeeld een project zich aan moet houden om te borgen dat beveiligingsmaatregelen niet vergeten worden bij het opstellen van specificaties.
- Is er aandacht voor om de behoeftesteller of de eigenaar van een systeem vooraf te betrekken bij het bepalen van de beveiligingseisen?
- Is er expertise nodig om te beoordelen of de ICT-dienstverlener voldoet aan de gestelde beveiligingsnormen voordat het contract gesloten wordt.

- Is er een goede test of keuringsmethodiek om te bepalen of aan de verplichte beveiligingseisen is voldaan.
- Maak gebruik van collega gemeenten die een vergelijkbare aanbesteding gedaan hebben en evalueer soortgelijke aanbestedingen.

Enkele aandachtspunten voor de juiste beveiligingseisen in contracten:

- Zijn de risico's geïdentificeerd in relatie tot de inkoop van diensten of goederen?
- Is de waarde en de gevoeligheid van de gegevens voor de afsluiting van een contract vastgesteld?
- Is de leverancier in staat om aan de gestelde beveiligings- en privacy vereisten te voldoen? Wat is de levensvatbaarheid van de leverancier (belangrijk wanneer diensten/gegevens bij de leverancier gehost/verwerkt worden)
- Worden er (bijzondere) persoonsgegevens gebruikt, is de bewerkersovereenkomst van toepassing?
- Welke beveiligingseisen vloeien voort uit wet- en regelgeving (bijvoorbeeld Wbp, BRP, BIG) of andere contracten/bestaande systemen (denk aan aansluitvoorwaarden)? Gelden daarnaast vereisten vanuit het interne privacy/security beleid?
- Is er aandacht voor privacybescherming? En zijn daartoe passende technische en organisatorische maatregelen geformuleerd richting de leverancier, als onderdeel van een bewerkersovereenkomst of contract?
- Waar bevindt de data van de gemeente zich (inclusief de back-up en de mirror).
- Zijn er beschikbaarheidseisen en is er een SLA nodig?
- Zijn de beveiligingseisen meetbaar voorafgaand aan en gedurende de contractperiode?
- Wordt er gebruik gemaakt van buitenlandse dienstverleners? Zo ja, welk recht is van toepassing?
- Zijn er speciale koppelvlakken voorzien, bijvoorbeeld voor koppelen met andere gemeenten, toegang voor beheerders van de leverancier of toegang door gemeentemedewerkers over niet vertrouwde netwerken?
- Zijn er bestaande generieke voorzieningen met ingebouwde beveiliging die gebruikt kunnen worden?
- Wordt er software ontwikkeld voor de gemeente:
    - Wie controleert de broncode, op welk moment en wat zijn de kwaliteitseisen?
    - Waar wordt deze software ontwikkeld?
    - Zijn er afspraken nodig om toch later over de broncode te kunnen beschikken door middel van een Escrow?
- Wordt er gebruik gemaakt van Cloud-diensten en waar bevinden die zich?
- Zijn er ontbindende voorwaarden in geval van een bedrijfsovername?
- Is er een exit-strategie? Ga bewust om met het risico van vendor lock-in en stel bij het sluiten van de overeenkomst maatregelen vast om het migreren van data en diensten mogelijk te maken. Denk daarbij niet alleen aan de situatie waarbij de gemeente het contract wilt beëindigen, of waarbij het van rechtswege afloopt, maar ook aan situaties als faillissement of wanprestatie aan de kant van de leverancier.
- Wat gebeurt er met de gegevens als deze niet meer een derden worden gebruikt.
- Is de leverancier NEN/ISO 27001 gecertificeerd? (dit is geen harde eis maar helpt wel bij het bepalen of de leverancier aandacht heeft voor informatiebeveiliging).

2.3 Wat te doen tijdens het lopende contract

Bij lopende contracten krijgt men ook te maken met beveiligingseisen die in contracten of de onderliggende SLA en/of bewerkersovereenkomst kunnen zitten. Met name gedurende de uitvoering van een contract gaat het om monitoren van de gemaakte afspraken, vaak is hier een samenspel van de contractmanager en de dienstafnemer voor nodig.

Aandachtspunten betreffende maatregelen die gedurende de looptijd van een contract nodig zijn:

- Zijn er audits afgesproken, worden die ook uitgevoerd en wat zijn daarvan de resultaten? Het kan bijvoorbeeld nodig zijn om in te grijpen als niet voldaan wordt aan de afgesproken eisen, als dit blijkt uit een audit?
- Is de leverancier verplicht om jaarlijks een Derdenverklaring of Third Party Mededeling (TPM) of een audit verklaring te overleggen? Wat doet de gemeente als deze TPM niet wordt overlegd?
- Is de leverancier verplicht om beveiligingsincidenten tijdig te melden aan de gemeente? Welke beveiligingsincidenten zijn er de afgelopen meetperiode opgetreden en welke contractafspraken worden geraakt door die incidenten?
- Er is een meldplicht voor datalekken en worden deze datalekken ook tijdig aan de gemeente en andere belanghebbenden gemeld, zodat de gemeente als verantwoordelijke ook tijdig de melding kan doen aan de Autoriteit persoonsgegevens?
- Zijn er belangrijke wijzigingen in de programmatuur of infrastructuur van de leverancier waardoor de beveiligingsafspraken geraakt worden? Hoe moet de leverancier de gemeente informeren?
- Worden de personele afspraken nagekomen door de leverancier?
- Zijn er wijzigingen aan de kant van de gemeente die van invloed zijn op de afspraken die met leveranciers gemaakt zijn? Hoe moet de gemeente de leverancier informeren?
- Worden de servicelevel rapportages tijdig opgeleverd en kloppen de rapportages met de afgesproken servicelevels?

2.4 Het beëindigen van contracten

Ook bij het beëindigen van contracten zijn er beveiligingsmaatregelen waar men rekening mee moet houden, met name als het gaat om dienstverlening die wordt overgedragen, bijvoorbeeld: insourcing of outsourcing, maar ook beëindigen van de dienstverlening. Een goede exit-strategie is belangrijk, om het risico van *vendor lock-in* te kunnen mitigeren.

De volgende aandachtspunten zijn er met betrekking tot contractbeëindiging en dienen al vooraf in de contracteringsfase te worden meegenomen voor het beëindigen van contracten.

Geheimhouding
Blijft geheimhouding van kracht ná het overdragen of beëindigen van de dienst? Dit dient in het contract en/of de bewerkersovereenkomst meegenomen te worden.

Vernietigen data

Data van de gemeente die op systemen staan van een derde partij dient zo spoedig mogelijk nadat deze data niet meer nodig is vernietigd te worden volgens aanwijzingen van de gemeente[1]. Deze vernietiging van data dient verantwoord en gecontroleerd te worden.

Migratie van de dienst

Bij het migreren van een dienst kunnen verschillende zaken verhuizen tussen dienstaanbieders of tussen de dienstaanbieder en de gemeente (insourcing/outsourcing). Denk hierbij aan processen, hardware, software en gegevens. De dienstaanbieder kan zowel een leverancier als een collega gemeente zijn. Denk daarbij aan het risico dat applicaties niet zonder meer overdraagbaar zijn van het ene naar het andere systeem. Dit kan migratie van diensten complex, tijdrovend en kostbaar maken.

Overdragen data en of software

Er moet aandacht zijn voor het overdragen van data en/of software tussen dienstenaanbieders van de gemeente. De nieuw gecontracteerde en latende leverancier verklaren zich op voorhand bereid tot het overdragen en ontvangen van data en/of software. Denk daarbij aan het risico dat gegevens niet zonder meer overdraagbaar zijn tussen applicatie of systeem.

[1] Meestal zal de gegevens eigenaar dit bepalen. Zie hiervoor bijvoorbeeld het document afvoer ICT-middelen waar verschillende vernietig mogelijkheden worden behandeld.

Bijlage: Contractmanagement beleid gemeente <gemeente>

Ten behoeve van de beveiliging van informatie is er contractmanagement beleid. Het doel van dit beleid is aanvullende eisen te stellen aan contractmanagement met als doel bescherming van gemeentelijke informatie en software te beveiligen.

De gemeente <naam gemeente> hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de BIG en aanvullend op het algemene beveiligingsbeleid van de gemeente:

Identificatie van risico's die betrekking hebben op externe partijen

De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd.

1. Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.

2. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.

3. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.

4. Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthenticeerde en geautoriseerde toegang vastgesteld wordt.

5. Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform WBP artikel 14) afgesloten.

6. Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.

7. Er wordt jaarlijks gerapporteerd over het naleven van de afspraken van de externe partij

Het beoordelen van beveiliging in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden beoordeeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.
Alle noodzakelijke beveiligingseisen worden op basis van een risicoafweging vastgesteld en geïmplementeerd, voordat aan gebruikers toegang tot informatie op bedrijfsmiddelen wordt

verleend.

Het behandelen van beveiliging in overeenkomsten met een derde partij

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen.

1. De maatregelen behorend bij de vastgestelde risico's zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.

2. Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin onder andere intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, Escrow en reviews geregeld worden.

3. In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.

4. In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.

5. Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit. Daarbij wordt rekening gehouden met verschillende scenario's (beeindiging contract, faillissement leverancier, wanprestatie).

6. In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.

7. In contracten met externe partijen is vastgelegd hoe de gemeente de afspraken mag controleren, bijvoorbeeld door middel van audits, en welke termijnen daar voor gelden.

8. Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.

9. De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum]*

[Naam. Functie] [Naam. Functie]

_____ _____

INFORMATIE BEVEILIGINGS DIENST

**INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82**

**INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN