TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Contractmanagement

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Contractmanagement’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt een handreiking voor het inrichten van beveiligingseisen bij contractmanagement voor organisaties binnen de Rijksoverheid. Deze uitgangspunten zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

Doelgroep

Dit document is van belang voor de directie van de organisatie, inkopers, contractmanagers en ICT-afdelingen.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregelen 6.2.1 en 6.2.3 van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- Inkoopvoorwaarden

Inhoudsopgave

1 Inleiding

Deze handreiking is geschreven om informatiebeveiligingsmaatregelen, die te maken hebben met contractmanagement, uit te werken. In de Baseline Informatiebeveiliging Rijksdienst (BIR) zijn een aantal maatregelen beschreven die te maken hebben met de omgang met externe partijen en contracten met derden. Een voorbeeld hiervan is de bewerkersovereenkomst die nodig is bij het bewerken van persoonsgegevens door een derde partij. Met de beschreven beveiligingseisen uit de BIR heeft een overheidsorganisatie een normenkader in handen om beveiligingseisen en -wensen die nodig zijn in contracten met derden uit te werken.

1.1 Doel van dit document

Het doel is dat contractmanagers, of diegene die te maken krijgt met contracten met derden, weten welke informatiebeveiligingsaspecten en welke omgang met gevoelige gegevens een rol spelen bij het uitvoeren van het contractmanagement.

Dit document gaat uit van de rol van contractmanager. Niet iedere organisatie heeft hiervoor een aparte functionaris in dienst, en de vergelijkbare taken kunnen ook door een andere rol in de organisatie worden uitgevoerd. De contracten kunnen ook worden beheerd binnen de ICT-afdeling, door een financiële afdeling of bijvoorbeeld door een afdelingshoofd. Dit document niet tot doel het gehele contractmanagement of gelinieerd inkoopproces te beschrijven.

1.2 Leeswijzer

Hoofdstuk 2 van dit document gaat in op de informatiebeveiligingsaspecten die een rol spelen bij contractmanagement. In de bijlage wordt een voorbeeld gegeven van aanvullend contractmanagementbeleid voor een organisatie binnen de Rijksoverheid.

2 Contractmanagement en informatiebeveiliging

2.1 Inleiding

Contractmanagement wordt hier begrepen als het proces dat er (onder meer) voor zorgt dat contracten worden beheerd. De taken die de contractmanager uitvoert, zijn onder andere:

- het opstellen, aangaan en nakomen van contracten;
- aansturen van de leveranciersrelatie;
- bewaken en vergroten van kwaliteit van de dienstverlening die wordt geleverd;
- voeren van contractonderhandelingen;
- handhaven van de overeengekomen contractsbepalingen.

Informatieveiligheid hoort een van de onderdelen van contracten met derden te zijn.
Een contractmanager dient de in contracten vastgelegde voorwaarden ten aanzien van informatiebeveiliging te bewaken.

In dit hoofdstuk wordt beschreven hoe om te gaan met informatiebeveiliging in contracten met derden voordat het contact gesloten is, tijdens de looptijd van het contract en bij het beëindigen van een contract.

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 eisen en wensen ten aanzien van beveiliging in het contract.

Wanneer er bijvoorbeeld persoonsgegevens, waar een overheidsorganisatie zeggenschap over heeft, in systemen bij een derde partij terecht kunnen komen, dienen voor de beveiliging maatregelen worden getroffen. Een van de maatregelen die moet worden genomen, is het afsluiten van een bewerkersovereenkomst. In deze bewerkersovereenkomst zitten alle eisen en wensen opgenomen die te maken hebben met de integriteit en exclusiviteit van de persoonsgegevens. Een van die te nemen maatregelen kan het versleutelen van de persoonsgegevens zijn. Een ander voorbeeld is dat een systeem wordt gebruikt voor processen die moeten voldoen aan bepaalde beschikbaarheidseisen. Deze beschikbaarheidseisen moeten worden vertaald naar contractuele voorwaarden en de Service Level Agreement (SLA) met de derde partij.

Waaraan moet gedacht worden voorafgaand aan een inkoopproces:

- Is er binnen de organisatie beleid of een stappenplan beschreven om te borgen dat de juiste beveiligingsmaatregelen worden opgenomen in het contract met derden?
- Om vast te stellen wat de juiste beveiligingsmaatregelen zijn, worden de volgende activiteiten uitgevoerd:
    - een verkorte risicoanalyse of baselinetoets;
    - eventueel een Privacy Impact Assessment (PIA);
    - een volledige risicoanalyse.

- Is er een formeel proces beschreven waarin wordt geborgd dat projecten beveiligingsmaatregelen meenemen bij het opstellen van specificaties?
- Is er voldoende aandacht in het inkoopproces voor het betrekken van de behoeftesteller of de eigenaar van een systeem bij het opstellen van beveiligingseisen?
- Is de juiste expertise beschikbaar voor het beoordelen of een 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?
- Wordt er geleerd van soortgelijke aanbestedingen bij vergelijkbare organisaties?

De volgende aandachtspunten dienen te worden meegenomen bij het opstellen van de juiste informatiebeveiligingseisen 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 privacyeisen te voldoen?
- Wat is de levensvatbaarheid van de leverancier (belangrijk wanneer diensten/gegevens bij de leverancier gehost/verwerkt worden)?
- Worden er persoonsgegevens verwerkt? In dergelijke gevallen is een bewerkersovereenkomst van toepassing?
- Welke beveiligingseisen vloeien voort uit wet- en regelgeving (bijvoorbeeld Wbp, BIR) of andere contracten of bestaande systemen (denk aan aansluitvoorwaarden)? Gelden daarnaast vereisten vanuit het interne privacy- en beveiligingsbeleid?
- Is er aandacht voor privacybescherming? En zijn daartoe passende technische en organisatorische maatregelen geformuleerd richting de leverancier?
- Waar bevindt de data van de organisatie 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 het koppelen met andere overheidsorganisaties, toegang voor beheerders van de leverancier of toegang door medewerkers over niet vertrouwde netwerken?
- Zijn er bestaande generieke voorzieningen met ingebouwde beveiliging die gebruikt kunnen worden?
- Wordt er software ontwikkeld voor de overheidsorganisatie?:
  - 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 bevindt de data zich in de cloud?
- Zijn er ontbindende voorwaarden in geval van een overname van de leverancier?

- Is er een exit-strategie? Ga bewust om met het risico van een zogenaamde *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 overheidsorganisatie het contract wilt beëindigen of waarbij het van rechtswege afloopt, maar ook aan onvoorziene situaties als faillissement of wanprestatie aan de kant van de leverancier.
- Wat gebeurt er met de gegevens als deze niet meer door derden worden gebruikt?
- Is de leverancier NEN/ISO 27001 gecertificeerd? Dit hoeft geen formele eis te zijn, maar kan dienen als waarborg voor informatiebeveiliging door de leverancier.

2.3 Wat te doen tijdens een lopend contract?

Gedurende de looptijd van een contract is het monitoren van de gemaakte afspraken het voornaamste. Vaak is hier een samenspel van de contractmanager en de dienstafnemer voor nodig. Bij lopende contracten dient ook rekening te worden gehouden met beveiligingseisen die in contracten of de onderliggende SLA en/of bewerkersovereenkomst kunnen zitten.

De volgende aandachtspunten betreffende beveiligingsmaatregelen dienen te worden meegenomen gedurende de looptijd van een contract:

- Zijn er audits afgesproken, worden die audits uitgevoerd en wat zijn daarvan de resultaten? Het kan bijvoorbeeld nodig zijn om de uitvoering van het contract bij te sturen als niet voldaan wordt aan de afgesproken eisen, zoals kan blijken uit een audit.
- Is de leverancier verplicht om jaarlijks een Third Party Mededeling (TPM) te overleggen, waarin een onafhankelijke auditer over de kwaliteit van een ICT-dienst rapporteert? Wat doet de organisatie als deze TPM niet wordt overlegd?
- Is de leverancier verplicht om beveiligingsincidenten tijdig te melden aan de organisatie? Welke beveiligingsincidenten zijn er de afgelopen meetperiode opgetreden en welke contractafspraken worden geraakt door die incidenten?
- Is er een meldplicht voor datalekken en worden deze datalekken ook tijdig aan de organisatie en andere belanghebbenden gemeld?
- Zijn er belangrijke wijzigingen in de programmatuur of infrastructuur van de leverancier waardoor de beveiligingsafspraken geraakt worden? Hoe moet de leverancier de overheidsorganisatie informeren?
- Worden de personele afspraken nagekomen door de leverancier?
- Zijn er wijzigingen aan de kant van de overheidsorganisatie die van invloed zijn op de afspraken die met leveranciers gemaakt zijn? Hoe moet de leverancier worden geïnformeerd?

2.4 Wat te doen bij het beëindigen van een contract?

Ook bij het beëindigen van contracten zijn er beveiligingsaspecten waarmee rekening gehouden moet worden, met name als de dienstverlening wordt overgedragen door middel van insourcing of outsourcing. Een goede exit-strategie is belangrijk bij het aflopen van een contract om het risico van *vendor lock-in* te kunnen mitigeren.

De volgende aandachtspunten zijn er met betrekking tot informatiebeveiliging bij een contractbeëindiging. Deze aandachtspunten dienen al in de contracteringsfase te worden meegenomen.

Geheimhouding

Blijft de geheimhouding contractueel 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 overheidsorganisatie 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 overheidsorganisatie.[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 overheidsorganisatie (bv. insourcing/outsourcing). Dit kan hardware, software en data betreffen. Bij migratie dient in acht genomen te worden dat applicaties niet zonder meer over te dragen zijn tussen verschillende systemen. Dit kan migratie van diensten complex, tijdrovend en kostbaar maken.

De nieuwe aanbieder van een dienst kan zowel een leverancier als een andere overheidsorganisatie zijn.

Overdragen data en software

Er moet bij het beëindigen van een contract aandacht zijn voor het eventuele overdragen van data en/of software tussen de oude en nieuwe dienstenaanbieders van de organisatie. De oude leverancier en de nieuw gecontracteerde leverancier verklaren zich op voorhand bereid tot het overdragen en ontvangen van data en/of software. Houd rekening met de mogelijkheid dat gegevens niet zonder meer overdraagbaar zijn tussen applicaties of systemen.

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

Bijlage: Contractmanagement beleid <organisatie>

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

De <organisatie> hanteert de volgende beleidsuitgangspunten die zijn ontleend aan de BIR en die aanvullend zijn op het algemene informatiebeveiligingsbeleid.

Identificatie van risico's die betrekking hebben op externe partijen

De risico's voor de informatie en ICT-voorzieningen van de organisatie door 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 of netwerk) 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 omgegaan dient te worden 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 (beëindiging 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 organisatie 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 de directie van *[organisatie]* op *[datum]*

[Naam. Functie] [Naam. Functie]

_____ _____