

BEWERKERSOVEREENKOMST

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



Colofon

Naam document

Bewerkersovereenkomst.

Versienummer

1.2

Versiedatum

April 2016

Versiebeheer

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

Copyright

© 2014 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de KING;
4. ieder kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan

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

Wijzigingshistorie:

Versie	Datum	Opmerkingen
1	18-02-2014	Eerste versie van de BIG
1.2	11-04-2016	Aanpassingen, lijst met met voorbeeld maatregelen aangepast.

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.

De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie 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.

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 geldt:

- 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

Dit product bevat een standaard bewerkersovereenkomst en een voorbeeld bijlage met maatregelen voor de bewerker die de gemeente als verantwoordelijke kan gebruiken bij het laten bewerken van persoonsgegevens.

Doelgroep

Dit document is van belang als de gemeente persoonsgegevens laat beheren door een derde partij, bijvoorbeeld bij een SaaS oplossing. Doelgroep is personen die te maken hebben met het uitbesteden van diensten waar persoonsgegevens worden bewerkt, bijvoorbeeld inkopers, contractbeheerders en systeemeigenaren.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
 - o Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
 - o Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
- Voorbeeld Informatiebeveiligingsbeleid van de gemeente, H2.4.1
- Beveiligingseisen in inkoopvoorwaarden
- Uitbesteding ICT-diensten
- Voorbeeld Responsible Disclosure beleid gemeenten

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 6.2.1.5 Afsluiten bewerkersovereenkomst

Maatregel 6.2.1.6 Vastleggen beveiligingsmaatregelen in contracten

Maatregel 6.2.1.7 Rapporteren over naleving van afspraken

Inhoud

1	Inleiding	6
2	Model bewerkersovereenkomst	9
2.1	Algemeen	9
2.2	Aansprakelijkheid	9
3	Bijlage 1: Maatregelen op basis van de BIG behorende bij bewerkersovereenkomst tussen gemeente <naam gemeente> en bewerker <bewerker>	16

1 Inleiding

Bij het uitbesteden van de verwerking van persoonsgegevens worden door de Wet bescherming persoonsgegevens (Wbp) nadere eisen gesteld, zie Art. 14 Jo 12 en 13 Wbp. Uit deze artikelen volgt dat de verantwoordelijke¹ (in dit geval de gemeente) een schriftelijke overeenkomst dient af te sluiten met de bewerker² (in dit geval de derde partij), deze overeenkomst heet de bewerkersovereenkomst.

De bewerker wordt door de Wbp gedefinieerd als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.'

Het opstellen van een bewerkersovereenkomst dient ertoe te waarborgen dat de verplichtingen die vanuit de Wbp op de verantwoordelijke rusten, ook door de bewerker worden nageleefd. Daartoe dienen in de bewerkersovereenkomst afspraken en maatregelen te staan die de verantwoordelijke genomen wil hebben door de bewerker. Belangrijk is dat volgens de Wbp de verantwoordelijke aanspreekbaar blijft voor de gegevens die onder zijn verantwoordelijkheid door de bewerker worden verwerkt.

Voorbeelden van bewerkers zijn:

- externe leveranciers, waaronder Cloud-dienst leveranciers
- adviseurs
- accountants
- EDP-auditors
- (salaris) administrateurs.

Hoewel het lijkt dat bijvoorbeeld een SaaS³ leverancier niet feitelijk de persoonsgegevens bewerkt, is deze toch volgens de Wbp de bewerker van persoonsgegevens als die op zijn / haar systemen staan.

Relatie met andere overeenkomsten

Het uitbesteden van werkzaamheden, de eigenlijke dienstverlening, wordt meestal in een aparte overeenkomst geregeld, hierna aangeduid met 'hoofdovereenkomst'.

De bewerkersovereenkomst regelt alleen het zorgvuldig omgaan met de persoonsgegevens die noodzakelijkerwijze bij de uitvoering van de 'hoofdovereenkomst' moeten worden verwerkt. Dat het beschermen van persoonsgegevens in een aparte overeenkomst moet worden geregeld, volgt uit de navolgende formulering de 'Memorie van Toelichting' (Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, p. 99): "De overeenkomst tussen de verantwoordelijke en de bewerker moet naar zijn aard betrekking hebben op de gegevensverwerking. Het contract mag geen betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is." Het is wel mogelijk de bewerkersovereenkomst apart op te stellen en vervolgens als bijlage op de hoofdovereenkomst op te nemen, waarbij in de hoofdovereenkomst naar deze bijlage wordt verwezen.

¹ De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

² De Wbp definieert de bewerker als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen' (Art. 1 sub e Wbp).

³ Zie: het document van de IBD over Cloud Computing gemeenten

Als de verantwoordelijke een bewerker inschakelt dient er op basis van de Wbp een schriftelijke overeenkomst te zijn, of dienen er vergelijkbare schriftelijke afspraken te bestaan: de zogenaamde 'bewerkersovereenkomst'. De bewerkersovereenkomst kan zelfstandig worden gebruikt maar is meestal een onderdeel van een overeenkomst met een breder bereik.⁴

De aspecten die in een (bewerker)overeenkomst moeten worden opgenomen en duidelijk moeten zijn:

- Wie de verantwoordelijke is en wie de bewerker is.
- Welke (soort) persoonsgegevens worden verwerkt en eventueel de wettelijke basis.
- Welke verwerkingen de bewerker precies moet doen. Hierbij kan ook geregeld worden wat de bewerker (in ieder geval) niet mag doen.
- De bewerker mag de persoonsgegevens uitsluitend bewerken in opdracht van de verantwoordelijke. De bewerker mag dus niet zelfstandig besluiten om, in afwijking van die opdracht, de persoonsgegevens op een bepaalde manier te verwerken. Tenzij een wettelijke verplichting dat vereist.
- Dat de bewerker zelfstandig aansprakelijk is voor schade die door de bewerker is veroorzaakt en hem kan worden toegerekend. En, eventueel, dat in geval de verantwoordelijke aansprakelijk gehouden wordt voor verwerkingen van de bewerker, de verantwoordelijke een regresrecht heeft (vrijwaringsbepaling).
- Dat de bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke dient daartoe instructies te geven, en dient toe te zien op naleving van die maatregelen.
- Wanneer een bewerker buiten de Europese Economische Ruimte (EER) gevestigd is, dient de verantwoordelijke ervoor zorg te dragen dat de bewerker het recht van het land van de verantwoordelijke nakomt (Art. 14 lid 4 Wbp).
- Dat de verantwoordelijke de mogelijkheden heeft om te controleren dat de bewerker zich (geheel) aan de overeenkomst houdt. Dit kan ook worden aangetoond met bijvoorbeeld een Third Party Memorandum (TPM), waarbij de verantwoordelijke de mogelijkheid van controle heeft.

De verantwoordelijke dient duidelijk aan de bewerker aan te geven welke maatregelen hij vereist voor het beschermen van de persoonsgegevens⁵. Deze maatregelen zijn voornamelijk gericht op exclusiviteit (vertrouwelijkheid) en integriteit van de gegevens van de verantwoordelijke, de beschikbaarheidseisen worden doorgaans in de SLA opgenomen.

De Autoriteit Persoonsgegevens (AP)⁶ biedt een aantal handreikingen ten behoeve van het opstellen van de bewerkersovereenkomst:

- Hoofdstuk 5 van de Handreiking verwerking persoonsgegevens:
<http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html>
- De Richtsnoeren beveiliging van persoonsgegevens, paragraaf 4.2 en paragraaf 4.3:
https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

⁴ zie hiervoor het document Inkoop voorwaarden en beveiligingseisen van de IBD

⁵ Zie bijvoorbeeld: De Richtsnoeren beveiliging van persoonsgegevens, paragraaf 4.2 en paragraaf 4.3 (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf)

⁶ Voorheen het College Bescherming Persoonsgegevens (CBP)

Ook is er meer informatie te vinden over afspraken die gemaakt kunnen worden in het volgende document van Enisa, wat ook over Cloud Computing en serviceniveau's gaat. In de Annex en bijlage staan vragen die gesteld kunnen worden:

<https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts>

2 Model bewerkersovereenkomst

2.1 Algemeen

Dit model is een voorbeeld van een bewerkersovereenkomst. Uiteraard is het niet het enige mogelijke model en is het denkbaar dat overeenkomsten meer of andere bepalingen bevatten die eveneens aan de Wbp voldoen.

Deze modelovereenkomst bevat generieke bepalingen die betrekking hebben op het naleven van de Wbp door de bewerker en niet op het naleven van andere wet- en regelgeving met betrekking tot persoonsgegevens, zoals de BRP- en SUWI-wetgeving. Uit deze wetgeving kunnen specifieke eisen voortvloeien, die in dit model niet zijn meegenomen.

Houd in gedachten dat verwerkingen die bijvoorbeeld vanwege de aard van de persoonsgegevens of de verwerkingen zelf met hogere waarborgen omkleed dienen te worden, niet in dit model vervat zijn.

Deze bewerkersovereenkomst is gebaseerd op de BIG, en is tot stand gekomen op basis van voorbeelden van onder meer de gemeente Amsterdam en een aantal leveranciers.

De bijlage bevat een selectie van BIG-maatregelen die onderwerp kunnen zijn van de bewerkersovereenkomst. De bijlage is een minimum variant en kan worden gezien als een startpunt en deze gaat uit van een generiek product of dienst zonder teveel achter de voordeur te kijken van de leverancier. De invulling en nadere specificatie is aan de gemeente zelf. Bij twijfel kan bijvoorbeeld ook een risicoanalyse worden uitgevoerd.

De overeenkomst is nu generiek opgezet, echter er kunnen verschillende persoonsgegevens in verschillende systemen staan, waarmee de generieke eisen dus ook niet overal van toepassing hoeven te zijn. Bedenk wel dat de gemeenten uiteindelijk allemaal ergens aan elkaar hangen en dat sommige gegevens die uit ketens afkomstig zijn, minimaal beveiligd moeten worden met eenzelfde niveau aan maatregelen tegen de risico's die er zijn.

Deze bewerkersovereenkomst is ook te gebruiken als algemeen model met afspraken tussen de gemeente en een leverancier.

2.2 Aansprakelijkheid

Over aansprakelijkheid (artikelen 9.1 tot en met 9.3 bewerkersovereenkomst) ontstaat vaak discussie en in dat verband is het belangrijk in te gaan op wat de Wbp daarover zegt in artikelen 49 en 50:

Artikel 49, derde lid, bepaalt dat de verantwoordelijke aansprakelijk is voor niet-naleving van de regels, door wie dan ook. Zou blijken dat de bewerker fouten heeft gemaakt dan kan de verantwoordelijke vervolgens de bewerker aanspreken. Daarnaast is de bewerker zelfstandig aansprakelijk voor eigen handelen. Beiden kunnen dus worden aangesproken door iemand die meent te zijn benadeeld bij de verwerking van zijn gegevens. Slechts wanneer verantwoordelijke of bewerker kunnen aantonen dat hun de schade niet kan worden aangerekend, gaan zij, blijkens het vierde lid, vrijuit.

De bepaling impliceert dus dat ook indien er een bewerker is die gegevens verwerkt ten behoeve van een verantwoordelijke, ook steeds die verantwoordelijke daarvoor aansprakelijk is. De verwerking blijft immers altijd onder de verantwoordelijkheid van de verantwoordelijke plaatsvinden. Daarnaast is de bewerker ook zelfstandig aansprakelijke voor zijn aandeel in de schade.

Bovengenoemde bepalingen uit de wet zijn dwingend recht en afwijkende bepalingen in overeenkomsten zijn nietig.

De leverancier is in de praktijk verantwoordelijk voor het uitvoeren van de technische maatregelen die nodig zijn voor het beveiligen van ICT. Juist door het aansprakelijk stellen voor schade die ontstaat door gebrekkige beveiliging wordt de softwareleverancier verplicht om de geleverde programmatuur uitgebreid te testen op beveiligingslekken. Ook zou in een Service Level Agreement (SLA) kunnen worden afgesproken dat een ICT-dienstverlener waaraan de data van een organisatie wordt toevertrouwd de inspanning levert om deze zo goed mogelijk te beschermen. Met het accepteren van hieruit voortvloeiende aansprakelijkheid wordt een ICT-dienstverlener gedwongen om zich in te zetten voor het faciliteren van veilig ICT-gebruik.

De overeenkomst

Wet bescherming persoonsgegevens (Wbp) bewerkersovereenkomst van de gemeente <GEMEENTE> met de (nader in te vullen) bewerker

De <functie>. van de gemeente <GEMEENTE>, gevestigd te <GEMEENTE>, verder te noemen de verantwoordelijke, ten deze rechtsgeldig vertegenwoordigd door de <heer of mevrouw><persoonsnaam>.,

en

<Bedrijf, afdeling>, gevestigd te <plaatsnaam>, verder te noemen de bewerker, ten deze rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie> ,

verklaren te zijn overeengekomen een bewerkersovereenkomst als bedoeld in artikel 14, tweede lid, van de Wbp, tussen de Dienst <dienst> van de gemeente <GEMEENTE> namens, nader te noemen de verantwoordelijke en <nader in te vullen naam van de bewerker>, nader te benoemen de bewerker.

Definities

Artikel 1.

- 1.1 Bijlagen: aanhangsels bij deze overeenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze overeenkomst.
- 1.2 Normen en standaarden: de door de verantwoordelijke vastgestelde normen en standaards ter zake van methoden, technieken, procedures, projecten, productietekeningen en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de bewerker zullen worden gevolgd als vastgelegd in bijlage 2 <door gemeente bij te voegen>.
- 1.3 Verwerking van persoonsgegevens of het verwerken van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.
- 1.4 Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
- 1.5 Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
- 1.6 Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- 1.7 Betrokkene: degene op wie een persoonsgegeven betrekking heeft.
- 1.8 Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.
- 1.9 Ontvanger: degene aan wie de persoonsgegevens worden verstrekt.
- 1.10 Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.
- 1.11 Het College bescherming persoonsgegevens of het College: het College als bedoeld in artikel 51 van de Wbp.

- 1.12 Functionaris: de functionaris voor de gegevensbescherming als bedoeld in artikel 62 van de Wbp.
- 1.13 Voorafgaand onderzoek: een onderzoek als bedoeld in artikel 31 van de Wbp.
- 1.14 Verstrekken van persoonsgegevens:- het bekend maken of ter beschikking stellen van persoonsgegevens.

Ingangsdatum en duur

Artikel 2.

- 2.1 Deze overeenkomst gaat in op het moment van ondertekening en duurt voort zolang de bewerker als bewerker van persoonsgegevens optreedt in het kader van de door de verantwoordelijke ter beschikking gestelde persoonsgegevens voor <nader in te vullen omschreven doel>

Onderwerp van deze overeenkomst

Artikel 3.

- 3.1 De bewerker verwerkt persoonsgegevens in opdracht van de verantwoordelijke in het kader van de uitvoering van < contract, nummer>.
- 3.2 De bewerker verbindt zich om in het kader van die werkzaamheden de door de verantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.
- 3.3 Dat de Wbp aan de verantwoordelijke de plicht oplegt om ervoor zorg te dragen dat de bewerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.

Naleving wet- en regelgeving

Artikel 4.

- 4.1 Het College van Burgemeester en Wethouders van de gemeente <GEMEENTE> is verantwoordelijke in de zin van de Wbp.
- 4.2 De Dienst / sector / cluster <afdelingsnaam> van de gemeente <GEMEENTE> is namens de verantwoordelijke belast met het beheer van de binnen de Dienst / sector / cluster <afdelingsnaam> in beheer zijnde gegevensverwerkingen.
- 4.3 De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke, in overeenstemming met diens instructies.
- 4.4 De bewerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze overeenkomst komt nimmer bij de bewerker te berusten.
- 4.5 De bewerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De bewerker verwerkt persoonsgegevens slechts in opdracht van de Dienst / sector / cluster <afdelingsnaam> en zal alle redelijke instructies van de Dienst / sector / cluster <afdelingsnaam> dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.
- 4.6 De bewerker zal onmiddellijk bij het ontdekken van beveiligingsinbreuken of datalekken deze melden aan de verantwoordelijke, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 9.3 van deze overeenkomst.
- 4.7 De bewerker zal te allen tijde op eerste verzoek van de Dienst <.....> onmiddellijk alle van de Dienst <.....> afkomstige persoonsgegevens met betrekking tot deze bewerkersovereenkomst ter hand stellen.
- 4.8 De bewerker zal alle van de verantwoordelijke afkomstige persoonsgegevens met betrekking tot deze bewerkersovereenkomst op een nader te bepalen wijze vernietigen op het moment van beëindigen van deze overeenkomst, dan wel op uitdrukkelijk verzoek van de verantwoordelijke de gegevens te vernietigen op een nader te bepalen wijze.

- 4.9 De bewerker stelt de verantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.

Geheimhoudingsplicht

Artikel 5.

- 5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de bewerker, evenals de bewerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. De medewerkers van de bewerker tekenen hiertoe een geheimhoudingsverklaring.
- 5.2 Indien de bewerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de bewerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de bewerker de Dienst <.....> onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Beveiligingsmaatregelen

Artikel 6.

- 6.1 De bewerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de verantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onzorgvuldig, ondeskundig of ongeoorloofd gebruik. Tevens verklaart de bewerker zich te houden aan de normen en standaards van de verantwoordelijke, zoals beschreven in bijlage 1.
- 6.2 De verantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te doen controleren. De bewerker is verplicht de verantwoordelijke of controlerende instantie in opdracht van verantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.
- 6.3 De verantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de bewerker.
- 6.4 De bewerker verbindt zich om binnen een door de verantwoordelijke te bepalen termijn de verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de bewerker van deze overeenkomst. De verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.
- 6.5 Bewerker staat er voor in, de door de verantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verantwoordelijke te bepalen termijn uit te voeren.
- 6.6 De bewerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze overeenkomst.

Inschakeling derden

Artikel 7.

- 7.1 De bewerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van de verantwoordelijke.
- 7.2 De verantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze bewerkersovereenkomst.

- 7.3 De bewerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze bewerkersovereenkomst.

Wijziging overeenkomst

Artikel 8.

- 8.1 Wijziging van deze overeenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.
- 8.2 Zodra de samenwerking is beëindigd, vernietigt bewerker de persoonsgegevens die hij van de verantwoordelijke heeft ontvangen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. Deze vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.
- 8.3 Elk van de partijen is gerechtigd de overeenkomst met onmiddellijke ingang te beëindigen in geval van overmacht, waaronder mede begrepen een zodanige wijziging van wettelijke regels dat een verdere voortzetting van de overeenkomst niet kan worden verlangd.
- 8.4 Bij het beëindigen van de overeenkomst met onmiddellijke ingang, wordt in de brief aan de bewerker de reden van beëindiging vermeld.

Aansprakelijkheid

Artikel 9.

- 9.1 Indien de bewerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst kan verantwoordelijke hem in gebreke stellen. Bewerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de bewerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is bewerker in verzuim.
- 9.2 Bewerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de Wbp gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze overeenkomst bepaalde. Onverminderd de aanspraken op grond van wettelijke regels. Bewerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid. Bewerker is tevens aansprakelijk voor alle schade of nadeel voortvloeiende uit de door zijn werkzaamheid ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen.
- 9.3. OPTIONEEL: Indien bewerker enige in artikel <.....> genoemde verplichting(en) niet tijdig nakomt, is bewerker een boete verschuldigd, groot <.....> per <gebeurtenis, dag, week maand> zonder dat hiervoor een aanmaning of een voorafgaande verklaring nodig is. Deze boete is niet vatbaar voor verrekening en opschorting en laat het recht van verantwoordelijke op nakoming en schadevergoeding onverlet.

Toepasselijk recht

Artikel 10.

- 10.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Citeertitel

Artikel 11.

- 11.1 Deze overeenkomst kan worden aangehaald als 'Bewerkersovereenkomst uitvoering <.....>'.

Aldus in tweevoud opgesteld en getekend de dato

Namens de verantwoordelijke, de Dienst / Afdeling / cluster <afdelingsnaam> van de gemeente
<GEMEENTE>,

de

Namens de <nader in te vullen gegevens bewerker>
<nader in te vullen gegevens vertegenwoordiger bewerker, zoals genoemd in de aanhef>

3 Bijlage 1: Maatregelen op basis van de BIG behorende bij bestedingsovereenkomst tussen gemeente <naam gemeente> en besteder <besteder>

Deze bijlage is gevuld met een suggestie van gekozen maatregelen uit de BIG en kunnen ook worden uitgebreid of aangepast. Nadruk ligt op de integriteit en exclusiviteit van de gegevens, beschikbaarheidseisen horen bij voorkeur in een SLA thuis.

Deze maatregelen zijn uit de BIG afkomstig en waar mogelijk specifiek gemaakt voor de besteder. Deze maatregelen gaan uit van het niveau van de BIG. Als de gegevens van de verantwoordelijke hoger geclassificeerd zijn, een hogere risico inschatting hebben (bijzondere persoonsgegevens) of extra maatregelen nodig hebben uit specifieke wetgeving, dan dient deze bijlage te worden uitgebreid.

BIG Numme r	titel	Control	BIG tekst / maatregel	Maatregel besteder
6.1.5.1	Geheimho udingsove reekomst	Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie moeten worden vastgesteld en regelmatig worden beoordeeld.	[A] De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3. Daarnaast dienen personen die te maken hebben met Bijzondere Informatie een geheimhoudingsverklaring te ondertekenen, daaronder valt ook vertrouwelijke informatie. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	Medewerkers die te maken hebben met persoonsinformatie van de verantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.
6.1.8.2	Onafhanke lijke beoorde ling van informatie beveiliging	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.	[A] Periodieke beveiligingsaudits worden uitgevoerd in opdracht van het lijnmanagement.	Periodieke beveiligingsaudits (minimaal eens per twee jaar) worden uitgevoerd volgens afspraken met de verantwoordelijke.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
6.2.1.7	Identificatie van risico's die betrekking hebben op externe partijen	De risico's voor de informatie en IT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, moeten worden geïdentificeerd en er moeten geschikte beheersmaatregelen worden geïmplementeerd voordat toegang wordt verleend.	Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.	Over het naleven van de afspraken wordt jaarlijks gerapporteerd aan de verantwoordelijke.
6.2.3.1	Beveiliging behandelende in overeenkomsten met een derde partij	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, moeten alle relevante beveiligingseisen zijn opgenomen.	De maatregelen behorend bij 6.2.1 zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.	Maatregelen uit de bewerkersovereenkomst zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.
7.2.2.1	Labeling en verwerking van informatie	Er moeten geschikte, samenhangende procedures worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie in overeenstemming met het classificatiesysteem dat de organisatie heeft geïmplementeerd.	[A] De lijnmanager heeft maatregelen getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van gerubriceerde informatie.	De bewerker heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens.
8.1.1.2	Rollen en verantwoordelijkheid en	De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging moeten worden vastgesteld en gedocumenteerd in overeenstemming met het beleid voor informatiebeveiliging van de organisatie.	[A] Alle ambtenaren en ingehuurde medewerkers krijgen bij hun aanstelling hun verantwoordelijkheden ten aanzien van informatiebeveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging, welke zij bij de vervulling van hun dienst hebben na te leven, worden op een gemakkelijk toegankelijke plaats ter inzage gelegd. in overeenstemming met voorschriften maken deze deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijkheid van	Het personeel van de bewerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verantwoordelijke.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
			geldende regelingen en instructies.	
8.1.2.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers moeten worden uitgevoerd in overeenstemming met relevante wetten, voorschriften en ethische overwegingen, en moeten evenredig zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.	[A] Voor alle medewerkers (ambtenaren en externe medewerkers) is minimaal een recente Verklaring Omtrent het Gedrag (VOG) vereist. Indien het een vertrouwensfunctie betreft wordt ook een veiligheidsonderzoek (Verklaring van Geen Bezwaar) uitgevoerd.	Voor het bedrijf is minimaal een recente Verklaring Omtrent het Gedrag Rechtspersonen (VOG RP) vereist met punten die door de verantwoordelijke zijn aangedragen.
8.3.3.1	Blokking van toegangsrechten	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen moeten worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of moet na wijziging worden aangepast.	Zie 8.3.1.3	Toegangsrechten van medewerkers van de bewerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.
9.1.2.1	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.	Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
9.1.3.1	Beveiliging van kantoren, ruimten en faciliteiten	Er moet fysieke beveiliging van kantoren, ruimten en faciliteiten worden ontworpen en toegepast.	Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen.	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verantwoordelijke bevatten worden beveiligd opgeslagen.
10.3.1.1	Capaciteitsbeheer	Het gebruik van middelen moet worden gecontroleerd en afgestemd en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.	[A] De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheid eis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.	De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
10.6.1.2	Maatregel en voor netwerken	Netwerken moeten adequaat worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.	[A] Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
10.6.1.3	Maatregel en voor netwerken	Netwerken moeten adequaat worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.	[A] Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de bewerker en de verantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.
10.6.2.1	Beveiliging van netwerkdiensten	Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een bewerker.
10.8.2.2	Uitwisselingsovereenkomsten	Er moeten overeenkomsten worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten.	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de bewerker naar de verantwoordelijke.
10.8.3.1	Fysieke media die worden getransporteerd	Media die informatie bevatten moeten worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.	Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals: <ul style="list-style-type: none"> • versleuteling • bescherming door fysieke maatregelen, zoals afgesloten containers • gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • persoonlijke aflevering • opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes 	De bewerker neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: <ul style="list-style-type: none"> • Versleuteling. • Bescherming door fysieke maatregelen, zoals afgesloten containers. • Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering. • Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
10.10.1.1	Aanmaken auditlogbestanden	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen moeten worden vastgelegd in audit-logbestanden. Deze logbestanden moeten gedurende een overeengekomen periode worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	Van logbestanden worden rapportages gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden. De GBA logging kan bijvoorbeeld dagelijks nagelopen worden, evenals financiële systemen, controle van het Internet gebruik kan bijvoorbeeld per maand of kwartaal.	Door de bewerker worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden.
10.10.1.2	Aanmaken auditlogbestanden	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen moeten worden vastgelegd in audit-logbestanden. Deze logbestanden moeten gedurende een overeengekomen periode worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	Een logregel bevat minimaal: <ul style="list-style-type: none"> • een tot een natuurlijk persoon herleidbare gebruikersnaam of ID • de gebeurtenis (zie 10.10.2.1) • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis 	Een logregel bevat minimaal: <ul style="list-style-type: none"> • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID. • De gebeurtenis (zie 10.10.2.1). • Waar mogelijk de identiteit van het werkstation of de locatie. • Het object waarop de handeling werd uitgevoerd. • Het resultaat van de handeling. • De datum en het tijdstip van de gebeurtenis.
10.10.1.3	Aanmaken auditlogbestanden	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen moeten worden vastgelegd in audit-logbestanden. Deze logbestanden moeten gedurende een overeengekomen periode worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	[A] In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).	In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
10.10.2.1	Controle van systeemgebruik	Er moeten procedures worden vastgesteld om het gebruik van IT - voorzieningen te controleren. Het resultaat van de controleactiviteiten moet regelmatig worden beoordeeld.	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: <ul style="list-style-type: none"> • Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels • Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) • Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders. 	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: <ul style="list-style-type: none"> • Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). • Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.

INFORMATIE BEVEILIGINGS DIENST

BIG Numme r	titel	Control	BIG tekst / maatregel	Maatregel bewerker
10.10.3.3	Bescherming van informatie in logestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen inbreuk en onbevoegde toegang.	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
10.10.3.5	Bescherming van informatie in logestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen inbreuk en onbevoegde toegang.	[A] De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de verantwoordelijke. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
10.10.6.1	Synchronisatie van systeemklokken	De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.	Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.	Er worden maatregelen genomen om ervoor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.
11.4.2.1	Authenticatie van gebruikers bij externe verbindingen.	Er moeten geschikte authenticatiemethoden worden gebruikt om toegang van gebruikers op afstand te beheersen.	Zie ook 11.6.1.3.	Als externe toegang nodig is tot de persoonsgegevens van de verantwoordelijke door eigen personeel, of personeel van de bewerker, dienen geschikte authenticatie methodes te worden gebruikt.
11.4.5.5	Scheiding van netwerken	Groepen informatiediensten, gebruikers en informatiesystemen moeten op netwerken worden gescheiden.	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
11.5.1.1	Beveiligde inlogprocedures	Toegang tot besturingssystemen moet worden beheerst met een beveiligde inlogprocedure.	[A] Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.	Toegang tot de persoonsgegevens van de verantwoordelijke wordt verleend op basis van twee-factor authenticatie.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
11.5.1.2	Beveiligde inlogprocedures	Toegang tot besturingssystemen moet worden beheerst met een beveiligde inlogprocedure.	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
11.5.1.3	Beveiligde inlogprocedures	Toegang tot besturingssystemen moet worden beheerst met een beveiligde inlogprocedure.	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
11.5.1.4	Beveiligde inlogprocedures	Toegang tot besturingssystemen moet worden beheerst met een beveiligde inlogprocedure.	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
11.5.1.5	Beveiligde inlogprocedures	Toegang tot besturingssystemen moet worden beheerst met een beveiligde inlogprocedure.	[A] Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.	Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.
11.5.2.1	Gebruikers identificatie en - authenticatie	Elke gebruiker moet over een unieke identificatiecode beschikken (gebruikers-ID) voor persoonlijk gebruik, en er moet een geschikte authenticatietechniek worden gekozen om de geclaimde identiteit van de gebruiker te verifiëren.	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.
11.5.3.1	Systemen voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
11.5.5.1	Time-out van sessies	Inactieve sessies moeten na een vastgestelde periode van inactiviteit worden uitgeschakeld.	[A] De periode van inactiviteit van een workstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.	De periode van inactiviteit van een workstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.
11.5.6.1	Beperking van verbindingstijd	De verbindingstijd moet worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.	[A] De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding. Met 2-factor authenticatie en tunneling.	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.
11.6.1.1	Beperking van toegang tot informatie	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel moet worden beperkt in overeenstemming met het vastgestelde toegangsbeleid.	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
11.6.1.2	Beperking van toegang tot informatie	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel moet worden beperkt in overeenstemming met het vastgestelde toegangsbeleid.	[A] Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
11.6.1.3	Beperking van toegang tot informatie	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel moet worden beperkt in overeenstemming met het vastgestelde toegangsbeleid.	[A] Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
12.1.1.1	Analyse en specificatie van beveiligingseisen	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen moeten ook eisen voor beveiligingsmaatregelen worden opgenomen.	In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.	In projecten ten behoeve van systemen voor de verantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
12.2.1.1	Validatie van invoergegevens	Gegevens die worden ingevoerd in toepassingen moeten worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.
12.2.2.1	Beheersing van interne gegevensverwerking	Er moeten validatiecontroles worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
12.2.3.1	Integriteit van berichten	Er moeten eisen worden vastgesteld, en geschikte beheersmaatregelen worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.	Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.	Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
12.2.4.1	Validatie van uitvoergegevens	Gegevensuitvoer uit een toepassing moet worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door check-sums).	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door check-sums).
12.3.1.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	Er moet beleid worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
12.3.2.1	Sleutelbeheer	Er moet sleutelbeheer zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
12.4.1.1	Beheersing van operationele software	Er moeten procedures zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.	Alleen geautoriseerd personeel kan functies en software installeren of activeren.	Alleen geautoriseerd personeel kan functies en software installeren of activeren.
12.5.1.1	Procedures voor wijzigingsbeheer	De implementatie van wijzigingen moet worden beheerst door middel van formele procedures voor wijzigingsbeheer.	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL en voor applicaties ASL.	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.
12.5.2.1	Technische beoordeling van toepassing en na wijzigingen in het besturingsstelsel	Bij wijzigingen in besturingssystemen moeten bedrijfskritische toepassingen worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen.	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de verantwoordelijke te niet doen.
12.5.4.1	Uitlekken van informatie	Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.	Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats.	Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats.
12.5.4.2	Uitlekken van informatie	Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.	Er dient een proces te zijn om te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)	Er dient een proces te zijn om aan de verantwoordelijke te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)
12.6.1.1	Beheersing van technische kwetsbaarheden	Er moet tijdig informatie worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten geschikte maatregelen worden	Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal het melden van incidenten aan de IBD, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
		genomen voor behandeling van daarmee samenhangende risico's.		
13.1.1.1	Rapportage van informatie beveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de verantwoordelijke vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
13.1.1.4	Rapportage van informatie beveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de IBD.	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verantwoordelijke.
13.1.1.5	Rapportage van informatie beveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Vermissing of diefstal van apparatuur of media die gegevens van de gemeente kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.	Vermissing of diefstal van apparatuur of media die gegevens van de verantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
13.2.3.1	Verzamelen van bewijsmateriaal	Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), moet bewijsmateriaal worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

INFORMATIE BEVEILIGINGS DIENST

BIG Nummer	titel	Control	BIG tekst / maatregel	Maatregel bewerker
		rechtsgebied zijn vastgelegd.		
15.1.3.1	Bescherming van bedrijfsdocumenten	Belangrijke registraties moeten worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.	Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.	De registraties van de verantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
15.1.4.1	Bescherming van gegevens en geheimhouding van persoonsgegevens	De bescherming van gegevens en privacy moet worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
15.1.6.1	Voorschrift en voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten in overeenstemming met alle relevante overeenkomsten, wetten en voorschriften worden gebruikt.	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.

INFORMATIE BEVEILIGINGS DIENST

BIG Numme r	titel	Control	BIG tekst / maatregel	Maatregel bewerker
15.2.1.1	Naleving van beveiligingsbeleid en -normen	Managers moeten bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.	Het lijnmanagement is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (o.a. jaarlijkse in control verklaring). Conform het BIG (strategisch kader) zorgt de CISO, namens de Gemeente Secretaris, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de CISO dan wel door interne of externe auditteams.	De bewerker is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze bewerkersovereenkomst en andere contractuele eisen zorgt de bewerker voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de verantwoordelijke.
15.2.2.1	Controle op technische naleving	Informatiesystemen moeten regelmatig worden gecontroleerd op naleving van implementatie van beveiligingsnormen.	Informatiesystemen worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijv. kwetsbaarheidsanalyses en penetratietesten. Zie ook 12.6.1.1.	Informatiesystemen van de bewerker ten behoeve van de verantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.

INFORMATIE BEVEILIGINGS DIENST

|

**INFORMATIEBEVEILIGINGSDIENST
VOOR 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**

**IBD@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL**



KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN