

Bijlage 1: Maatregelen op basis van de BIG behorende bij Bewerkersovereenkomst tussen Verantwoordelijke en Bewerker

De BIG, de Baseline Informatiebeveiliging Gemeenten, is het normenkader voor gemeenten. Omdat de Bewerker werkzaamheden uitvoert voor Verantwoordelijke, geldt deze norm waar relevant ook voor de Bewerker. De BIG is gebaseerd op zowel de ISO/NEN 27001 als 27002 en bestaat uit een strategisch, tactisch en operationeel deel.

De maatregelen in deze bijlage zijn een selectie uit de tactische BIG en specifiek gemaakt voor de Bewerker. De tactische BIG is gebaseerd op de ISO/NEN 27002. Nadruk in deze selectie ligt op de integriteit en exclusiviteit van de gegevens. Beschikbaarheidseisen zijn voornamelijk in de SLA opgenomen.

De BIG is een product van de IBD (Informatiebeveiligingsdienst voor gemeenten) een onderdeel van KING (Kwaliteitsinstituut Nederlandse Gemeenten). De gehele BIG en er aan gerelateerde producten zijn terug te vinden op de website van de IBD:

<https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/>

Toelichting tabel

Kolom	Omschrijving
Big nr	Referentie naar de tactische BIG.
Groep	Groep binnen het BIG-hoofdstuk waar deze maatregel bij hoort.
Control	Achtergrond van de maatregel.
Maatregel Bewerker	Vertaling van de maatregel voor de bewerker.
Eis	Geeft aan of aan de betreffende maatregel bij aanvang van de overeenkomst volledig (V) of deels (D) moet zijn voldaan. Bij "deels" zijn verbeterpunten toegestaan. Het is niet acceptabel als aan een maatregel helemaal geen invulling is gegeven. De Bewerker moet op termijn aan alle maatregelen volledig voldoen. Wanneer een specifieke (minimum) termijn geldt, is die bij de maatregel genoemd. Naar aanleiding van de jaarlijkse rapportage kunnen in overleg termijnen worden aangepast of aanvullend worden bepaald.

De Bewerker is transparant over de mate waarin aan de eisen wordt voldaan en laat dit door een onafhankelijke derde vaststellen en vastleggen in een rapportage. De Verantwoordelijke ontvangt van Bewerker een kopie van deze rapportage. Zie hiervoor ook maatregelen 6.1.8.2 en 6.2.1.7.

Beveiligingsbeleid

BIG nr	Groep	Control	Maatregel Bewerker	E
5.1.1.1	Beleidsdocument voor informatiebeveiliging	Een document met informatiebeveiligingsbeleid moet door de directie worden goedgekeurd en gepubliceerd en kenbaar worden gemaakt aan alle werknemers en relevante externe partijen.	De Bewerker heeft een eigen vastgesteld en gepubliceerd informatie beveiligingsbeleid.	V
5.1.2.1	Beoordeling van het informatiebeveiligingsbeleid	Het informatiebeveiligingsbeleid moet met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.	Het informatiebeveiligingsbeleid van de Bewerker wordt minimaal éénmaal per drie jaar of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.	V

Organisatie van informatiebeveiliging

BIG nr	Groep	Control	Maatregel Bewerker	E
6.1.4.1	Goedkeuringsproces voor IT-voorzieningen	Er moet een goedkeuringsproces voor nieuwe IT-voorzieningen worden vastgesteld en geïmplementeerd.	De Bewerker heeft een goedkeuringsproces voor nieuwe ICT-voorzieningen en wijzigingen in ICT-voorzieningen.	D
6.1.5.1	Geheimhoudings-overeenkomst	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.	Medewerkers die te maken hebben met persoonsinformatie van de Verantwoordelijke dienen (een arbeidsovereenkomst met daarin opgenomen) een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.	V
6.1.8.2	Onafhankelijke beoordeling van informatiebeveiliging	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.	Periodieke beveiligingsaudits (minimaal eens per jaar) worden uitgevoerd volgens afspraken met de Verantwoordelijke.	V
6.2.1.1	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.	Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.	V
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 wordt jaarlijks gerapporteerd aan de Verantwoordelijke. Uiterlijk zes weken voor de verlengdatum van de (hoofd) overeenkomst. En eerder waar er specifiekere momenten zijn afgesproken.	V

Beheer van bedrijfsmiddelen

BIG nr	Groep	Control	Maatregel Bewerker	E
7.1.3.1	Aanvaardbaar gebruik van bedrijfsmiddelen	Er moeten regels worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen.	Er zijn regels voor acceptabel gebruik van bedrijfsmiddelen (o.a. internet, e-mail en mobiele apparatuur). Met name worden er afspraken gemaakt omtrent werken op afstand en het gebruik van mobiele devices. Indien geen "werken op afstand" of vergelijkbaar beleid aanwezig is wordt dit minimaal 1 jaar na aangaan van deze overeenkomst opgesteld.	D

Personele beveiliging

BIG nr	Groep	Control	Maatregel Bewerker	E
8.1.1.2	Rollen en verantwoordelijkheden	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.	Het personeel van de Bewerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de Verantwoordelijke. Dit wordt bij voorkeur vastgelegd in de (arbeids) overeenkomst.	D
8.1.1.4	Rollen en verantwoordelijkheden	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.	De algemene voorwaarden van het (arbeids) contract van medewerkers of contractant bevatten de wederzijdse verantwoordelijkheden ten aanzien van beveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van (informatie)beveiliging.	D
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.	De Bewerker beschikt over een recente Verklaring Omtrent Gedrag RP (rechtspersoon) of voor de medewerkers die persoonsgegevens bewerken is een recente Verklaring Omtrent Gedrag aanwezig.	V
8.2.2.1	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Alle werknemers van de organisatie en, voorzover van toepassing, ingehuurd personeel en externe gebruikers, moeten geschikte training en regelmatige bijscholing krijgen met betrekking tot beleid en procedures van de organisatie, voorzover relevant voor hun functie.	Alle medewerkers van de Bewerker zijn regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de Bewerker, voor zover relevant voor hun functie.	D
8.3.3.1	Blokkering 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.	Toegangsrechten van medewerkers van de Bewerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.	V

Fysieke beveiliging

BIG nr	Groep	Control	Maatregel Bewerker	E
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 beveiligde zones of gebouwen waar persoonsgegevens van de Verantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.	V
9.2.7.1	Verwijdering van bedrijfseigendommen	Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.	Apparatuur, informatie en programmatuur met persoonsgegevens van de Verantwoordelijke mogen niet zonder toestemming vooraf van de locatie van de Bewerker worden meegenomen.	V

Beheer van communicatie en bedienprocessen

BIG nr	Groep	Control	Maatregel Bewerker	E
10.1.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd, worden bijgehouden en beschikbaar worden gesteld aan alle gebruikers die deze nodig hebben.	Bedieningsprocedures ten behoeve van de bewerking van persoonsgegevens van de Verantwoordelijke bevatten informatie over opstarten, afsluiten, back-up- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.	D
10.3.2.2	Systeem acceptatie	Security by Design wordt gerealiseerd door relevante standaarden en richtlijnen toe te passen.	Acceptatiecriteria voor het testen van de beveiliging betreft minimaal de meest recente OWASP top-10. De Bewerker toont aan dat de door Bewerker geleverde (web)applicatie geen kwetsbaarheden bevat uit de top-10.	V
10.6.1.3	Maatregelen 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.	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.	V
10.7.2.1	Verwijdering van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, in overeenstemming met formele procedures.	Het verwijderen cq. vernietigen van vertrouwelijke data en de vernietiging van verwijderbare media gebeurt conform landelijke wet- en regelgeving.	V
10.8.1.4	Beleid en procedures voor informatie-uitwisseling	Er moeten formeel beleid, formele procedures en formele beheersmaatregelen zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.	Medewerkers van de Bewerker zijn geïnstrueerd om geen vertrouwelijke documenten met informatie van de Verantwoordelijke bij de printer te laten liggen.	D
10.8.2.1	Uitwisselingsovereenkomsten	Er moeten overeenkomsten worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.	De Bewerker en de Verantwoordelijke hebben afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen de Bewerker en de Verantwoordelijke. Zie ook 10.6.1.3.	D
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 in de (bewerker-) overeenkomst.	V

BIG nr	Groep	Control	Maatregel Bewerker	E
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. 	D

Toegangsbeveiliging

BIG nr	Groep	Control	Maatregel Bewerker	E
11.1.1.1	Toegangsbeleid	Er moet toegangsbeleid worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.	De bewerker heeft een autorisatiebeleid.	V
11.2.1.1	Registratie van gebruikers	Er moeten formele procedures voor het registreren en afmelden van gebruikers worden vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.	De bewerker heeft een autorisatiebeleid.	V
11.2.1.3	Registratie van gebruikers	Er moeten formele procedures voor het registreren en afmelden van gebruikers worden vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.	Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	V

BIG nr	Groep	Control	Maatregel Bewerker	E
11.2.2.1	Beheer van speciale bevoegdheden	De toewijzing en het gebruik van speciale bevoegdheden moet worden beperkt en gecontroleerd.	Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (need to know, need to use).	V
11.3.1.1	Gebruik van wachtwoorden	Gebruikers moeten de goede beveiligingsgewoonten in acht nemen bij het kiezen en gebruiken van wachtwoorden.	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: <ul style="list-style-type: none"> • Wachtwoorden worden niet opgeschreven. • Gebruikers delen hun wachtwoord nooit met anderen. • Wachtwoorden mogen niet opeenvolgend zijn. • Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde. • Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro). Uitzondering zijn wachtwoordmanagers die met een sterk wachtwoord zijn beveiligd. 	V
11.5.2.2	Gebruikersidentificatie 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 het intern gebruik van ICT-voorzieningen worden gebruikers minimaal geauthentiseerd op basis van wachtwoorden.	V
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 (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).	D
11.7.1.1	Draagbare computers en communicatievoorzieningen	Er moet formeel beleid zijn vastgesteld en er moeten geschikte beveiligingsmaatregelen zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.	Het is de Bewerker niet toegestaan om mobiele apparaten te gebruiken voor het beheer van persoonsgegevens van de Verantwoordelijke.	V

Verwerking, onderhoud en ontwikkeling

BIG nr	Groep	Control	Maatregel Bewerker	E
12.1.1.2	Analyse en specificatie van beveiligingseisen	Security by Design wordt gerealiseerd door relevante standaarden en richtlijnen toe te passen.	De Beveiligingsrichtlijnen voor Webapplicaties van het NCSC worden toegepast bij analyse, ontwikkeling en testen van het informatiesysteem. Waar relevant worden ook andere standaarden en richtlijnen gebruikt.	V
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.	V
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 aan de Verantwoordelijke te melden dat (persoons) informatie is uitgelekt.	V

BIG nr	Groep	Control	Maatregel Bewerker	E
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 genomen voor behandeling van daarmee samenhangende risico's.	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.	V
12.6.1.4	Beheersing van technische kwetsbaarheden	Updates en patches moeten tijdig aangebracht zijn.	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiliging-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.	V

Beheer van incidenten

BIG nr	Groep	Control	Maatregel Bewerker	E
13.1.1.1	Rapportage van informatiebeveiligings gebeurtenissen	Informatiebeveiligingsgebeurtenissen en moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	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.	V
13.1.1.5	Rapportage van informatiebeveiligings gebeurtenissen	Informatiebeveiligingsgebeurtenissen en moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Vermissing of diefstal van apparatuur of media die gegevens van de Verantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.	V
13.2.2.1	Leren van informatiebeveiligings incidenten	Er moeten mechanismen zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.	De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren. (PDCA-Cyclus)	V

Naleving

BIG nr	Groep	Control	Maatregel Bewerker	E
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.	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.	D

BIG nr	Groep	Control	Maatregel Bewerker	E
15.2.2.1	Controle op technische naleving	Informatiesystemen moeten regelmatig worden gecontroleerd op naleving van implementatie van beveiligingsnormen.	Informatiesystemen van de Bewerker ten behoeve van de Verantwoordelijke worden regelmatig (minimaal 1x per jaar) gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.	V

ISMS

BIG nr	Groep	Control	Maatregel Bewerker	E
104.1.1.1	Algemene vereisten	<p>De organisatie dient een gedocumenteerd ISMS te ontwikkelen, te onderhouden en constant te verbeteren, binnen het kader van de bedrijfsactiviteiten en risico van de organisatie.</p> <p>Ten behoeve van deze standaard wordt het onderliggende proces gebaseerd op het PDCA model (Plan, Do, Check, Act).</p>	<p>De Bewerker is ISO 27001 gecertificeerd of heeft een BIG certificaat/TPM waarmee aangetoond wordt dat een gedocumenteerd ISMS is ontwikkeld, wordt onderhouden en constant verbeterd wordt, binnen het kader van de bedrijfsactiviteiten en risico van de organisatie.</p> <p>Ten behoeve van deze standaard wordt het onderliggende proces gebaseerd op het PDCA model (Plan, Do, Check, Act).</p>	D