Oplegvel Collegebesluit

Portefeuille weth. Divendal
Auteur dhr. M. van der Plas/P. Jongkees
Telefoon 5113073 E-mail: mplas@haarlem.nl
DV/BB Reg.nr. 2009/117858
GEEN bijlagen kopiëren
B & W-vergadering van 12 januari 2010

Onderwerp
Informatiebeveiligingsplan GBA en waardedocumenten

DOEL: Besluiten
Het informatiebeveiligingsplan GBA en waardedocumenten gaat deel uitmaken van een overkoepelend gemeentelijk informatiebeveiligingsplan. Veel maatregelen die nu voor de GBA zijn uitgewerkt zullen dan algemeen gelden voor alle gemeentelijke basisregistraties, zoals de Basisregistratie voor Adressen en Gebouwen (BAG).

Het College van burgemeester en wethouders is wettelijk verantwoordelijk voor het vaststellen van het informatiebeveiligingsplan GBA en Waardedocumenten.
Met het Informatiebeveiligingsplan GBA en waardedocumenten wordt uitvoering gegeven aan de artikelen 1 en 2 van de verordening GBA over de verstrekking van persoonsgegevens aan binnen- en buitengemeentelijke afnemers.

Bij het bespreken van de verordening GBA en waardedocumenten in de commissie Bestuur is aangegeven dat de raad geïnformeerd wordt over de uitvoeringsregels die het college stelt. Dit kan geregeld worden door toezending van het informatiebeveilingsplan inclusief privacyreglement+ bijbehorende bijlagen 1 tot en met 4. De overige bijlagen van het informatiebeveiligingsplan liggen ter inzage bij de griffie. Wij stellen voor een paar bijlagen niet ter inzage te leggen omdat deze uit beveiligingsoptiek geheim zijn (bijvoorbeeld uitwijk- en back-upprocedures). In dit soort specifieke gevallen wringt de wens van transparantie richting gemeenteraad met het beveiligingsbelang!

Omdat er nogal wat discussie/vragen waren over dit onderwerp, is het voorstel om de stukken ter bespreking aan de commissie Bestuur aan te bieden en niet ter informatie.

Er wordt momenteel gewerkt aan het opstellen van een gemeentebreed informatiebeveiligingsplan. Daarbij komt ook het onderwerp privacy aan de orde. Als er opmerkingen zijn van de commissie Bestuur kunnen deze als input fungeren bij het opstellen van het gemeentebrede informatiebeveiligingsplan inclusief privacyreglement.

B&W
1. Het college besluit het Informatiebeveiligingsplan GBA en Waardedocumenten inclusief het privacyreglement GBA en alle daarbij behorende bijlagen vast te stellen
2. Het besluit van het college incl. het informatiebeveiligingsplan GBA en Waardedocumenten inclusief privacyreglement+ bijbehorende bijlagen 1 tot en met 4. wordt ter bespreking toegestuurd aan de commissie Bestuur. De overige bijlagen van het informatiebeveiligingsplan liggen ter inzage bij de griffie. Uit oogpunt van bedrijfsbelang worden geheime procedures (als uitwijk- en back-upprocedures) niet ter inzage gelegd.
3. De eventuele opmerkingen van de commissie Bestuur betreffende de onder 1. genoemde stukken mee te nemen als input bij het opstellen van het gemeentebrede informatiebeveiligingsplan inclusief privacyreglement.
4. Dit besluit heeft geen financiële consequenties.
5. De betrokkenen ontvangen daags na besluitvorming informatie over dit besluit

COLLEGEBESLUIT

Onderwerp: Informatiebeveiligingsplan GBA en Waardedocumenten

Inleiding

Met de invoering van de wet Basisregistratie personen per 1 januari 2010 is de Gemeentelijke basisadministratie personen (GBA) de enige authentieke bron voor persoonsgegevens voor de overheid.
De verplichte gebruikers van de GBA mogen een snelle en betrouwbare dienstverlening verwachten bij het gebruik van de GBA. De gemeente kan dit garanderen als duidelijk is welke risico's er zijn en als regelmatig de voorzorgsmaatregelen worden uitgevoerd om die risico's te beheersen. Daarvoor is het informatiebeveiligingsplan GBA en waardedocumenten opgesteld.

Bij het bespreken van de verordening GBA in de commissie Bestuur is aangegeven dat de raad geïnformeerd wordt over de uitvoeringsregels die het college stelt. Dit kan geregeld worden door toezending van het informatiebeveiligingsplan inclusief privacyreglement+ bijlagen. Omdat er discussie/vragen waren over dit onderwerp, is het voorstel om de stukken ter bespreking aan de commissie Bestuur aan te bieden en niet ter informatie. De overige bijlagen van het informatiebeveiligingsplan liggen ter inzage bij de griffie. Wij stellen voor een paar bijlagen niet ter inzage te leggen omdat deze uit beveiligingsoptiek geheim zijn (bijvoorbeeld uitwijk- en back-upprocedures). In dit soort specifieke gevallen wringt de wens van transparantie richting gemeenteraad met het beveiligingsbelang!

Er wordt momenteel gewerkt aan het opstellen van een gemeentebreed informatiebeveilingsplan. Daarbij komt ook het onderwerp privacy aan de orde. Als er opmerkingen zijn van de commissie kunnen deze als input fungeren bij het opstellen van het gemeentebrede informatiebeveiligingsplan inclusief privacyreglement. Indien noodzakelijk kunnen ook de regels rondom de GBA worden aangepast.

Besluitpunten college

1. Het college besluit het Informatiebeveiligingsplan GBA en Waardedocumenten inclusief het privacyreglement GBA en alle daarbij behorende bijlagen vast te stellen
2. Het besluit van het college incl. het informatiebeveiligingsplan GBA en Waardedocumenten inclusief privacyreglement+ bijbehorende bijlagen 1 tot en met 4. wordt ter bespreking toegestuurd aan de commissie Bestuur. De overige bijlagen van het informatiebeveiligingsplan liggen ter inzage bij de griffie. Uit oogpunt van bedrijfsbelang worden geheime procedures (als uitwijk- en back-upprocedures) niet ter inzage gelegd.
3. De eventuele opmerkingen van de commissie Bestuur betreffende de onder 1. genoemde stukken mee te nemen als input bij het opstellen van het gemeentebrede informatiebeveiligingsplan inclusief privacyreglement.
4. Dit besluit heeft geen financiële consequenties.
5. De betrokkenen ontvangen daags na besluitvorming informatie over dit besluit

Beoogd resultaat
De in het voorliggend Informatiebeveiligingsplan GBA en Waardedocumenten opgenomen procedures dekken de risico's bij de verwerking van persoonsgegevens af.

Argumenten
De wettelijke regelingen voor GBA, BAG, privacy en waardedocumenten (paspoorten, rijbewijzen) stellen eisen aan de informatiebeveiliging.
Deze eisen betreffen de betrouwbaarheid van de GBA. Dit plan garandeert een betrouwbare GBA doordat de beschikbaarheid, data integriteit, vertrouwelijkheid en controleerbaarheid van de GBA worden geborgd in de bedrijfsprocessen en de dienstverlening. Het informatiebeveiligingsplan is opgesteld door bureau BMC in overleg met de eigen organisatie. Dit extern bureau ondersteunt minimaal de helft van de gemeenten voor dit onderwerp. Juist gelet op het belang van dit onderwerp is bij de implementatie externe expertise betrokken om een kwaliteitsplan GBA te maken.

De aanwezigheid van een gemeentelijk informatiebeveiligingsplan GBA en Waardedocumenten is wettelijk verplicht en wordt getoetst bij de verplichte landelijke GBA audit in het eerste kwartaal 2010.

Kanttekeningen
In artikel 2 van de verordening GBA is bepaald dat het college van BenW nadere regels kan stellen voor de verstrekking van persoonsgegevens aan binnen- en buitengemeentelijke afnemers. Deze regels zijn vervat in een pricacyreglement dat onderdeel is van dit informatiebeveiligingsplan.

Dit privacyreglement is samengesteld aan de hand van een model van bureau BMC. Voor het benoemen van de binnen- en buitengemeentelijke afnemers die gegevens uit het GBA kunnen krijgen, is aangesloten bij het landelijk referentiemodel van de Nederlandse Vereniging van Burgerzaken. Enige verschil is dat is geschrapt wat niet voor de gemeente Haarlem van toepassing is. Het is overigens mogelijk om desgewenst de lijst verder aan te passen en bijv. partijen uit te sluiten.

In de bijlagen wordt vermeld welke binnen – en buitengemeentelijke afnemers informatie kunnen krijgen. Het feit dat deze partijen in de bijlagen worden vermeld, betekent overigens niet dat zij automatisch de gegevens ook krijgen. Er vindt eerst een toets plaats op basis van twee apart beschreven procedures die in het informatiebeveiligingsplan zijn verwerkt. Dit is overigens een uitvoering in de vorm van een werkinstructie voor de medewerkers van hetgeen in de wet GBA is vastgelegd. Altijd wordt daarbij een belangenafweging gemaakt of het doel en de omvang van de vraag gegevensverstrekking rechtvaardigt uit oogpunt van privacy.
Er worden twee soorten aanvragers onderscheiden:
a. verstrekkingen aan natuurlijke personen.
b. verstrekkingen aan rechtspersonen zonder winstoogmerk

ad a. Bij natuurlijke personen wordt pas informatie verstrekt als betrokkene daarvoor schriftelijk uitdrukkelijk toestemming heeft gegeven.

ad b. Criteria die bij de belangenafweging/toetsing worden aangehouden:
1. Is de verstrekking noodzakelijk in belang van bescherming van betrokkene of van rechten en vrijheden van anderen?
2. Is er een dringende maatschappelijke behoefte?
3. Staat verstrekking in verhouding tot het doel van de aanvraag?

4. Kan het doel niet op minder ingrijpende wijze worden bereikt?
Gegevensverstrekking vindt alleen plaats als alle vier vragen positief worden beantwoord.

De gegevensverstrekking betreft –conform de wet GBA- niet meer dan de telefoonboekgegevens. Als betrokkene geheimhouding heeft laten registreren in de GBA worden gegevens in deze categorie altijd geweigerd.
Het is dus niet zo dat de zgn. vrije derden automatisch recht op gegevens hebben. Overigens komt het in de praktijk niet of nauwelijks voor dat kerken, sportverenigingen e.d. om informatie verzoeken. Het aantal aanvragen van rechtspersonen is doorgaans beperkt. Het betreft meestal bewindvoerders en Jeugdzorg. De voorgestelde procedure is op basis van de modellen van BMC en in lijn met de wet- en regelgeving (wet GBA).

Het besluit heeft geen financiële consequenties.

Uitvoering
Op een systematische manier beschrijft dit plan de risico's en de voorzorgsmaatregelen. Op basis van een jaarplanning en normenstelsel worden de voorzorgsmaatregelen getest en gemeten op effectiviteit. Werkt een voorzorgsmaatregel onder de maat dan onderneemt de beheerorganisatie GBA actie om het gewenste beveiligingsniveau te herstellen. Het Informatiebeveiligingsplan GBA en Waardedocumenten maakt onderdeel uit van de interne controle om de werking van het informatiebeveiligingsbeheer objectief te kunnen beoordelen.

Bijlagen
Het informatiebeveiligingsplan GBA en Waardedocumenten (incl bijlagen).

Het college van burgemeester en wethouders

Informatiebeveiligingsplan

GBA en Waardedocumenten

Gemeente Haarlem

Versie : Burgemeester en wethouders

Status : Goedgekeurd door directie

Auteur : mevrouw W.A.A.M. Zwanenburg

Datum : 14 december 2009

Bestuur en Management Consultants (BMC)

Inhoudsopgave

1 Algemeen

1.1 Inleiding

In de gemeentelijke organisatie is een toenemend gebruik van geautomatiseerde informatiesystemen te constateren. In het algemeen zijn de gebruikers van deze systemen zich onvoldoende bewust van de risico's die worden gelopen ten aanzien van een ongestoord gebruik hiervan. Meestal zeer onverwachts kan zich een calamiteit voordoen, die het geautomatiseerde proces danig kan verstoren.

Voorliggend Informatiebeveiligingsplan is bedoeld om de risico's, verbonden aan het toenemend gebruik van computersystemen, zichtbaar te maken en aan te geven hoe deze risico's maximaal kunnen worden ingeperkt.

In dit Informatiebeveiligingsplan zijn de uitgangspunten en beveiligingsprocedures opgenomen, die invulling geven aan al deze eisen.

1.2 Goedkeuring

Goedkeuring van de in dit document opgenomen beveiligingsprocedures vindt plaats nadat de betrokken personen van zowel de opdrachtnemer als opdrachtgever overeenstemming hebben bereikt over wat in het Informatiebeveiligingsplan staat beschreven.

Voor accordering van het voorliggend Informatiebeveiligingsplan tekent hieronder de opdrachtgever:

Gemeente Haarlem

College van B&W

Postbus 511

2003 PB Haarlem

Burgemeester, de heer mr. B.B. Schneiders

Plaats en datum: Haarlem, december 2009

Handtekening:

Gemeentesecretaris, de heer drs. W.J. Sleddering

Plaats en datum: Haarlem, december 2009

Handtekening:

1.3 Versiebeheer

Versie	Datum	Auteur	Status	Aard wijzigingen	Verstuurd aan
0.1	12 december 2008	Mevrouw W.A.A.M. Zwanenburg	concept	1e concept	aghpjonkers@haarlem.nl
0.2	26 januari 2009	Mevrouw W.A.A.M. Zwanenburg	concept	Administratieve aanpassingen	aghpjonkers@haarlem.nl
0.3	4 maart 2009	Mevrouw W.A.A.M. Zwanenburg	concept	Administratieve aanpassingen	aghpjonkers@haarlem.nl
1.0			definitief		

1.4 Overleggroep Informatiebeveiliging GBA en waardedocumenten

Ten behoeve van de totstandkoming van en periodieke afstemming (minimaal tweemaal per jaar) over voorliggend Informatiebeveiligingsplan is door de gemeente Haarlem een (permanente) overleggroep Informatiebeveiliging GBA en waardedocumenten ingesteld.

Deze overleggroep Informatiebeveiliging GBA en waardedocumenten bestaat uit de volgende medewerkers:

- De gegevensbeheerder GBA
- Het afdelingshoofd Informatie en Communicatie Technologie
- De beveiligingsbeheerder
- De teammanager Bedrijfsbureau
- De applicatiebeheerder GBA
- De beveiligingsfunctionaris reisdocumenten/rijbewijzen
- De applicatiebeheerder ICT

1.5 Geïnterviewden

Ten behoeve van de totstandkoming van het voorliggend Informatiebeveiligingsplan zijn op 12 december 2008 de volgende personen geïnterviewd:

- De gegevensbeheerder GBA
- De beveiligingsbeheerder
- De applicatiebeheerder ICT
- De locatiebeheerder Facilitaire Zaken
- De adviseur Dienstverlening, namens de manager Dienstverlening

De geïnterviewden hebben of een sleutelrol in het beheer van de kernapplicatie GBA, of in het beheer van waardedocumenten, of in de (fysieke) beveiliging van het gemeentehuis.

1.6 Verantwoording

Voorliggend Informatiebeveiligingsplan is gebaseerd op de normen zoals vastgesteld in de Code voor Informatiebeveiliging. De Code is gebaseerd op de beste praktijkmethoden voor informatiebeveiliging zoals internationaal gebruikt in vele toonaangevende bedrijven.

Daarnaast is het voorliggend Informatiebeveiligingsplan gebaseerd op de in de aparte hoofdstukken opgenomen regelgeving.

1.7 Jaarlijkse actualisering

Het Informatiebeveiligingsplan en de aangedragen en genomen beveiligingsmaatregelen worden jaarlijks geëvalueerd en eventueel bijgesteld door de overleggroep Informatiebeveiliging GBA en waardedocumenten en vervolgens rechtstreeks aangeboden ter advisering aan de directie. Daarna

wordt het geactualiseerde Informatiebeveiligingsplan aangeboden ter vaststelling aan het college van B&W.

1.8 Uitvoering en evaluatie

Informatiebeveiliging is pas effectief als deze op een gestructureerde manier wordt aangepakt. De basis hiervoor is de Beleidsdoelstelling van het informatiebeveiligingsbeleid. Binnen de organisatie moeten medewerkers verantwoordelijkheden krijgen voor de implementatie van dit beleid.

De medewerkers worden betrokken (o.a. tijdens werkoverleg) bij de ontwikkeling en implementatie van zowel het beleid als de uitvoering.
Daarnaast moet door de beveiligingsbeheerder worden vastgesteld of de maatregelen worden nageleefd. Verder verdient het aanbeveling minimaal eenmaal per jaar het beleid te evalueren en eventueel te herzien.
Het voorliggend Informatiebeveiligingsplan bevat tevens een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden bezien op actualiteit. In het Informatiebeveiligingsplan zijn daarom afspraken vastgelegd over de verantwoordelijkheid voor handhaving en naleving van de getroffen maatregelen en procedures. De belangrijkste afspraak in dit verband is dat het voorliggend Informatiebeveiligingsplan jaarlijks opnieuw moet worden bekeken op actualiteit en dat de wijzigingen worden vastgesteld door het college van B&W, waarbij tevens wordt gecontroleerd op naleving van de beleidsuitgangspunten. Hiervoor is per maatregel voorzien in een rapportage door de daartoe aangewezen medewerker. Zie hiervoor de Bijlage Functieverdeling.
Daarnaast dient het gehele beleid minimaal eenmaal per raadsperiode te worden herijkt.

2 Beveiliging

2.1 Waarom beveiligen?

De dagelijkse taakuitoefening wordt steeds meer beheerst door het gebruik van computers. Daarbij ontstaat informatie die van wezenlijk belang is voor het functioneren van de gemeentelijke organisatie.

De gemeentelijke organisatie is als gevolg van deze ontwikkeling in toenemende mate afhankelijk van een ongestoorde werking van haar informatiesystemen. Informatiesystemen zijn langzamerhand het zenuwcentrum geworden van de gemeentelijke organisatie.

Dat wordt gekarakteriseerd door:

- Probleemloos samenwerken van medewerkers op verschillende locaties.
- Het steeds groter worden van gegevensverzamelingen.
- De snelheid waarmee gegevens kunnen worden verwerkt.
- De (on)leesbaarheid voor de mens van vastgelegde gegevens.
- De éénmalige vastlegging ten behoeve van meerdere toepassingen en gebruikers.
- Concentratie van specifieke (informatiserings)kennis bij enkelen.

De kwetsbaarheid van deze gemeentelijke informatiesystemen is dan ook een groot risico, waarvan de gemeentelijke organisatie zeer nadelige gevolgen kan ondervinden. Het is dus zaak door middel van zowel preventieve als repressieve beveiligingsmaatregelen de risico's zoveel mogelijk te beperken.

Maar het zijn niet slechts interne redenen waarom de gemeente haar informatievoorziening moet beveiligen. Ook de wetgever stelt een aantal eisen. Door de Wet bescherming persoonsgegevens (WBP) worden eisen gesteld, die aan gemeenten worden verplicht gesteld en die zich richten tegen "verlies of enige vorm van onrechtmatige verwerking van gegevens". Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot *alle* onderdelen van het proces van gegevensverwerking.

De gemeente moet in het kader van de WBP "passende" beveiligingsmaatregelen nemen. In het begrip "passend" ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens.

Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van gegevens.

2.2 Wat beveiligen?

De functie van een informatiesysteem kan worden omschreven als het vastleggen, opslaan en verwerken van gegevens en het verstrekken van informatie. Beveiliging heeft daarom niet alleen betrekking op de hardware, maar ook op het gebruik ervan.

Ergo, de computerbeveiliging richt zich op de volgende beveiligingsobjecten:

- Hardware en supplies.
- Software.
- Gegevens (data).
- Datacommunicatie.
- Systeem- en applicatiedocumentatie.
- Het gebouw (het gemeentehuis inclusief locaties).
- Werkplek.
- Het eigen personeel.

De middelen die ten aanzien van deze beveiliging worden ingezet richten zich op het voorkómen, het ontdekken en het herstellen van de schade. De schade kan van materiële of immateriële aard zijn. De schade kan per ongeluk zijn ontstaan of opzettelijk zijn toegebracht.

Logische informatiebeveiliging is geen op zichzelf staande inspanning, doch maakt deel uit van de complete beveiliging. Een aantal maatregelen ligt dan ook in het verlengde van de al geldende beveiligingsmaatregelen, in het bijzonder waar deze betrekking hebben op de fysieke beveiliging van het gebouw en de werkplek.

In het kader van de Gemeentelijke Basisadministratie zijn ten aanzien van de veiligheid van gegevens hoge eisen gesteld. Om aan die eisen tegemoet te kunnen komen, dient, met respect voor de eigen omgeving, het beheer adequaat te zijn ingericht. Het begint ermee dat de eigen processen aan een stevige analyse worden onderworpen. De analyse is er op gericht dat de bedreigingen in beeld worden gebracht. Vervolgens moet de kans op optreden van die bedreigingen zo effectief mogelijk naar een zo laag mogelijk niveau worden gebracht.

Beveiliging van gegevens vraagt om zorgvuldige analyses van de risico's die met die gegevens samenhangen. Gegevens kunnen verloren gaan, verminkt en daardoor onbetrouwbaar worden en tenslotte in volledig verkeerde handen vallen.

Onder informatiebeveiliging wordt in dit kader verstaan een samenhangend geheel van maatregelen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens garandeert.

Teneinde te komen tot een zo verantwoord mogelijke toepassing van informatiesystemen in de gemeentelijke organisatie is het van essentieel belang via een stelsel van richtlijnen en procedures aan te geven hoe de beheerders en gebruikers dienen om te gaan met deze informatiesystemen.

In dit hoofdstuk wordt dieper ingegaan op de hoedanigheid van de verschillende beveiligingsobjecten.

2.2.1 Hardware

Onder hardware wordt verstaan:

- Server(s).
- Systeemconsole.
- Werkstations (inclusief beeldschermen, muis en toetsenbord).
- Laptops, PDA's, smartphones.
- Extern geheugen zoals vaste schijven en schijvenpakketten.
- Tape-unit.
- UPS.
- Patchkast met bekabeling.
- Randapparatuur zoals printers, plotter, CD-ROM spelers, tapestreamers, diskette units en paspoort- en rijbewijzenconfiguratie.
- Communicatieapparatuur.
- Supplies als tapes, cd's en diskettes.

De hardware lijkt zo op het oog een nogal kwetsbaar beveiligingsobject. In fysieke zin is dit ongetwijfeld juist. Wel moet worden bedacht dat de hardware, in tegenstelling tot de software, vrij snel vervangbaar is, waarna het verwerkingsproces kan worden hervat. Zo is er voor de RS6000 pSeries model 550 een (respons) onderhoudscontract afgesloten door de gemeente Haarlem. Zie hiervoor de Bijlage Onderhoudscontract.

Een andere mogelijkheid is om het verwerkingsproces bij calamiteiten tijdelijk voort te zetten op bij het uitwijkcentrum aanwezige identieke hardware. De gemeente Haarlem heeft hiervoor een uitwijkcontract gesloten met IBM te Almere.

2.2.2 Software

De gemeente heeft in verreweg de meeste gevallen standaard software aangeschaft. Daarom draagt de leverancier van de standaardprogrammatuur zorg voor beveiliging van de originele programmatuur. Bij calamiteiten kan de beschadigde of verloren software in principe altijd worden vervangen. Dit laat onverlet dat de programmatuur regelmatig moet worden beveiligd.

Er is geen sprake van een eigen systeemontwikkeling. Mocht dit plaatsvinden, dan is het belangrijk te beseffen dat verlies van software niet alleen desastreus is voor de beschikbaarheid van de werkzaamheden, maar ook, vanwege herprogrammering, belangrijke financiële nadelen kan opleveren. Voorkomen moet worden dat de software om welke reden dan ook verloren kan gaan.

De gemeente Haarlem gebruikt in het kader van voorliggend Informatiebeveiligingsplan op de RS6000 pSeries model 550 de applicatie Probev van de leverancier Procura.

2.2.3 Gegevens

Gegevens zijn over het algemeen voor iedere organisatie uniek. Indien gegevens om wat voor reden dan ook verloren gaan kan men, tenzij men maatregelen heeft genomen, nergens meer op terugvallen. Reconstrueren van gegevens (voor zover mogelijk) is een kostbare en tijdrovende aangelegenheid.

Het is daarom van het grootste belang dat de gegevens elke werkdag worden gekopieerd naar een back-up medium, zodat bij calamiteiten de operationele versie onmiddellijk kan worden vervangen door de laatst gemaakte kopie. De gebruikte methode voor het maken van een back-up is de zogenaamde generatiebeveiliging.

2.2.4 Datacommunicatie verbindingen

Onder verbindingen worden verstaan de communicatielijnen die verschillende computers onderling met elkaar verbinden. Vooral zodra het openbare telefoonnet als communicatiemedium wordt gebruikt loopt men het risico dat onbevoegden het informatiesysteem binnendringen. Voor hackers gaat op dit punt echt geen zee te hoog en het is een goede zaak daar ernstig rekening mee te houden. De enige afdoende beveiliging in deze situatie is de zogenaamde cryptografie, waarmee de over de communicatielijn te transporteren gegevens onleesbaar worden gemaakt voor onbevoegden. Voor het transport van bijvoorbeeld geheime data is cryptografie eigenlijk een "must". Bij het transport van andersoortige data kan worden gehandeld als bij een niet op een openbaar netwerk aangesloten informatiesysteem.

In computersystemen die niet zijn gekoppeld aan het openbare net is het gevaar van inbreuk door externe onbevoegden minder aanwezig. Toch dient ook in dit geval een stelsel van identificatiecodes en wachtwoorden te voorkomen dat interne onbevoegden het systeem kunnen binnendringen.

Internet is in principe toegankelijk via de op het locale netwerk aangesloten Pc's.

Beveiliging tegen hackers is gewaarborgd via een eigen firewall. Daarnaast wordt een extra beveiliging nagestreefd met behulp van de virusscanner Sophos anti-virus van Sophos. Zie hiervoor ook de Procedure Antivirus voorzieningen.

2.2.5 Documentatie

Onder documentatie wordt verstaan:

systeemdocumentatie

- Hierin staat het doel en de werking van het informatiesysteem beschreven. Het betreft het volgende:
    - Configuratiebeschrijving.
    - Bekabelingsplan.
    - Contracten met de leveranciers.
    - Systeemhandboeken.

- Aanwijzingen voor het onderhoud.
- De te nemen acties bij storingen.

gebruikersdocumentatie

- Hierin staat beschreven hoe de gebruiker dient om te gaan met de diverse applicaties. Deze documentatie wordt door de applicatieleverancier beschikbaar gesteld.
- Ook voor de zelf ontwikkelde applicaties geldt dat er documentatie aanwezig dient te zijn.

De verantwoordelijkheid voor het bijhouden van de systeemdocumentatie ligt bij het afdelingshoofd Informatie en Communicatie Technologie. De verantwoordelijkheid voor het bijhouden van de gebruikersdocumentatie ligt bij de applicatiebeheerder GBA.

2.2.6 Het gebouw

Het gemeentehuis van Haarlem is op een aantal manieren beveiligd. Er zijn voorzieningen getroffen ten behoeve van de fysieke beveiliging door de firma NVD Beveiligingen uit Haarlem. Hierbij is sprake van compartimentering van het gebouw. Tevens is er een inbraakwerende voorziening (stil alarm naar de meldcentrale van NVD Beveiligingen te Haarlem).

De zogenoemde kritische ruimten zijn afgesloten voor het publiek. In een gedeelte van het gemeentehuis zijn inbraakwerende voorzieningen getroffen in de vorm van bewegingsmelders. Er is een elektronische toegangsbeveiliging voor het gemeentehuis. Tijdens avondopenstellingen is er slechts in beperkte mate maar voldoende controle op de toegang van het gebouw.

Beveiliging wil in dit verband ook zeggen: ontruiming in geval van brand- en/of bommeldingen.

Fysieke beveiliging dislocaties
Er is in de gemeente Haarlem geen dislocatie.

Kritische ruimten
Een kritische ruimte is een ruimte waarin een kwaadwillige zoveel schade kan aanrichten dat de beschikbaarheid van de gemeentelijke werkprocessen kan worden verstoord. Een voorbeeld hiervan is de computerruimte.
De volgende ruimten worden als kritisch beschouwd:

- Ruimte systeem- en netwerkbeheer.
- Computerruimte inclusief het Raasstation en patchkast.
- Kluisruimte back-up.
- Kluisruimte waardedocumenten.
- Werkruimten.
- Spreekkamers.

Daarnaast is de volgende ruimte aangewezen die weliswaar niet bedrijfskritisch is maar wel extra beveiligd moeten worden. Dit omdat de werkzaamheden die er in worden uitgevoerd een groter diefstal en/of overvalrisico met zich meebrengen:

- Centrale kas.

2.2.7 Werkplek

De servers staan in een afzonderlijke afgesloten computerruimte die zoveel mogelijk stofvrij is en waar een vorm van luchtbehandeling wordt toegepast.

Uiteraard moet de computerruimte fysiek goed worden beveiligd. De werkplekken zelf (waar de werkstations staan) zijn fysiek minder goed te beveiligen. Hier moet worden teruggevallen op de algemene beveiligingsmaatregelen van gemeentelijke gebouwen.

De werkstations staan in de werkruimten en behoeven geen aparte luchtbehandeling.

2.3 Waartegen moet worden beveiligd?

2.3.1 Inleiding

Computers zijn uiterst verfijnde staaltjes van technisch vernuft en ze bestaan uit technische ingewikkelde apparatuur. Voor de gebruikers is het van groot belang dat kan worden vertrouwd op een ongestoorde werking. Er zijn organisaties die zo afhankelijk zijn geworden van hun informatiesystemen dat zij in hun voortbestaan bedreigd worden wanneer deze enige tijd niet zouden kunnen worden gebruikt (bijvoorbeeld door technische storingen of door brand).

Het voortbestaan van de gemeentelijke organisatie hangt voor een belangrijk deel af van computerinstallaties. Het staat vast dat de informatievoorziening ernstig zou zijn ontregeld als één of meer operationele informatiesystemen enige tijd niet zouden kunnen worden gebruikt (denk bijvoorbeeld aan het uitvallen van het informatiesysteem van Sociale Zaken met zijn berekenings- en betalingsruns of uitvallen van het GBA systeem met de daaraan gekoppelde dienstverlening naar de burger en landelijke afnemers).

Daar komt nog bij dat het belang van computers, de kwetsbaarheid ervan en de waarde die ze vertegenwoordigen, zo groot is dat dit soort installaties een uitermate geschikt doelwit zijn voor fraude, diefstal en sabotage. De ervaringen van enkele gemeenten in het verleden tonen aan dat dit niet louter theorie is.

Er kunnen diverse voorzorgsmaatregelen genomen worden die er voor kunnen zorgen dat het gevaar van grote stagnatie en extra kosten als gevolg van het uitvallen van een informatiesysteem tot een minimum wordt beperkt of zelfs wordt uitgesloten.

Een toenemende mate van afhankelijkheid van computers vraagt om een toenemende mate van beveiliging van die zelfde computers.

2.3.2 Bliksem, brand en explosie

Bliksem is een groot gevaar voor gebouwen. Een blikseminslag kan een spanning bereiken van enkele 100.000 Volt stroom tot een stroomsterkte van 200.000 Ampère. Deze elektrische energie wordt binnen 50 tot 100 seconden vrijgemaakt en weer afgevoerd. Een blikseminslag van deze kracht veroorzaakt binnen een straal van 2 kilometer spanningspieken in de elektrische bedrading die elektronische apparaten kunnen beschadigen. Deze spanningspiek neemt af naarmate de afstand tot de inslag groter is.
Wanneer een gebouw direct wordt getroffen door de bliksem kan door de vrijkomende dynamische energie het fundament worden beschadigd. Tevens kan brand uitbreken.

Brand is een reëel en altijd aanwezig gevaar, het is ook de meest voorkomende calamiteit. Brand kan fataal zijn voor gehele informatiesystemen. Naast directe schade kan vuur ook grote gevolgschade aanrichten. Het door de brandweer gebruikte bluswater beschadigt ook andere (veelal lager gelegen) delen van het door brand getroffen gebouw. De gebruikte apparatuur is hier erg gevoelig voor.
Bij de verbranding van het in kantoorpanden veel gebruikte PVC ontstaan chloorgassen die met het bluswater zoutzuurachtige verbindingen aangaan. Door het gebruik van klimaatbeheersingssystemen in kantoorpanden kunnen deze verbindingen door het gehele gebouw worden verspreid zodat ook de gevoelige elektronische apparatuur die ver van de brandhaard staat opgesteld, wordt aangetast.

2.3.3 Stof, vuil en water

Computers zijn bijzonder gevoelig voor stof. Voor servers geldt in het algemeen dat er maatregelen moeten worden genomen om de hoeveelheid aanwezige stof zoveel mogelijk te beperken. Een luchtbehandelinginstallatie is in dat geval onontbeerlijk. Voor PC's is dit in mindere mate het geval. Deze hardware is zo geconstrueerd dat er geen speciale voorzieningen nodig zijn.

Stofbeheersing blijft een belangrijk aspect ter voorkoming van storingen aan de hardware. Als gevolg van stof laten de filters in de koelelementen van computers steeds minder lucht door, waardoor de temperatuur op een gegeven moment te hoog kan oplopen. Regelmatig onderhoud is dus geboden. Bij verwisseling van media (tapes, cd's en diskettes) kan gemakkelijk stofinfiltratie plaatsvinden. Al met al redenen om zoveel mogelijk te werken in een schone omgeving.

De oplossing hiervan wordt zichtbaar door rekening te houden met de volgende aanbevelingen. De apparatuur moet dan op een zodanige wijze worden geplaatst en beveiligd dat de risico's van schade, storing en gebruik door stof, vuil en water minimaal zijn.

Dit wordt bereikt door:

- Aandacht voor specifieke risico's, waaronder water, stof, trillingen, chemische reactie, interferentie met de elektriciteitsvoorziening en elektromagnetische straling.
- Verbod tot gebruik van etenswaren in kritische ruimten.
- Iedere medewerker er voor verantwoordelijk te houden zijn of haar eigen werkplek zoveel mogelijk stofvrij te houden.
- Weer zoveel mogelijk stofbronnen, zoals kartonnen dozen en bloembakken in de nabijheid van computerapparatuur.

Water in de gevoelige ICT apparatuur is verantwoordelijk voor kortsluiting, mechanische beschadiging en/of roestvorming. Doordat in de meeste kantoorgebouwen de telefooncentrale, de computerapparatuur, patchkasten en de hoofdverdelers voor de interne stroomvoorziening zijn gecentraliseerd in één fysieke ruimte, betekent waterschade in deze ruimte onmiddellijk een enorme schade.

Ongecontroleerde toestroom van water kan worden veroorzaakt door:

- Hoog water.
- Storing in het water(afvoer) systeem.
- Defect van het verwarmingssysteem.
- Defect van het klimaatbeheersingssysteem (airco).
- Defect van een Sprinkler installatie.
- Bluswater van de brandweer.

2.3.4 Stroomuitval, storingen en fouten

Ondanks de verfijnde techniek en ondanks alle preventieve maatregelen kunnen er situaties ontstaan waarbij het informatiesysteem niet meer functioneert. Naast brand en explosie kunnen ook technische storingen de werking van het informatiesysteem ernstig verstoren.

Verfijnde apparatuur als netwerkservers zijn doorgaans gevoelig voor snelle temperatuurswisselingen. Vooral als het buiten heet is, kan veel apparatuur die is opgesteld in dezelfde computerruimte zijn warmte niet kwijt. De ruimte waar de computerhardware (servers/patchkast) staat is voorzien van airconditioning om een zo constant mogelijke temperatuur te waarborgen.

Ondanks de hoge kwaliteit van de Nederlandse stroomvoorziening, komt het toch op jaarbasis een aantal keren voor dat de stroom uitvalt. Meestal zal de stroomonderbreking niet langer duren dan een seconde zodat mensen het in het geheel niet opmerken. ICT apparatuur kan echter verstoord raken bij een stroomonderbreking langer dan 10 ms. Van stroomtoevoer zijn niet alleen de servers, PC's en verlichting afhankelijk, maar ook liften, buizenpost, telefoonapparatuur, beveiligingsapparatuur (brand en inbraak), airconditioning, verwarming en de watertoevoer in flats.
Storingen in de stroomvoorziening kunnen in principe worden ondervangen door het plaatsen van een zogenaamde UPS (Uninteruptible Power Supply) installatie. Hoewel dit een kostbare aangelegenheid is

en de kwaliteit van de geleverde elektriciteit in Nederland goed te noemen is, is de hardware (zeker de servers) zodanig storingsgevoelig dat een UPS een must is. Een UPS is te vergelijken met een flinke accu. Dankzij een UPS kan een server in geval van stroomuitval correct afgesloten worden.

Voor een doelmatige beveiliging is de duur van de 'down-time' van belang. Met down-time wordt bedoeld de tijd dat het informatiesysteem niet inzetbaar is. Is een langdurige systeemuitval van meer dan een paar dagen niet acceptabel, dan zal men moeten zorgen voor een "uitwijksysteem" op de werkplek zelf of in de directe nabijheid. In geval van de GBA moet de beschikbaarheid van de dienstverlening worden verzekerd naar de burger, de interne afnemers en de externe afnemers. Het is daarom wettelijk verplicht om voor de GBA een uitwijkcontract en een eigen uitwijkprocedure te hebben. Ook in de beveiligingseisen t.a.v. het gebruik van het DKD is een voorwaarde opgenomen op basis waarvan gestreefd moet worden naar een optimale continuïteit. Dit maakt een uitwijkvoorziening nodig.

Door defecten, verkeerde bediening, ondeskundige wijziging of manipulatie en/of stroomuitval kunnen allerlei fysieke beveiligingsvoorzieningen uitvallen:

- Defecte deursloten.
- Vervuilde brandmelders.
- Beschadigde sleutels of badges.
- Vastgeklemde regelcontacten in deuren.
- Ingebrande schermen van beveiligingsmonitoren.
- Modems en lijnverbindingen.

Dit soort problemen kunnen doorgaans niet worden opgelost door de gebruiker. Contact met de leverancier is in dat geval noodzakelijk.
Storingen aan de software kunnen een ernstig karakter krijgen als blijkt dat de software onverhoopt niet voorziet in bepaalde praktijksituaties. De enige vorm van beveiliging is hier een uitgebreide en diepgaande testperiode, voorafgaand aan de ingebruikneming van de software.
Een veel voorkomende groep van storingen wordt gevormd door printerstoringen. Deze zijn doorgaans snel oplosbaar, maar vormen een niet aflatende bron van irritaties voor de gebruikers.

2.3.5 Diefstal, sabotage, virussen en fraude door derden

Diefstal
Door de beperkte omvang van PC's en zeker laptops, is het voorkomen van diefstal van hardware een zaak geworden die wel degelijk aandacht verdient. Immers, een laptop is al in een aktetas mee te nemen. En wat te denken van opslagmedia als tapecassettes, diskettes en cd's. Hoewel dit geen dure apparatuur en/of opslagmedia betreft, zijn ze wel bruikbaar in de privé-sfeer.

Er zijn echter nog andere risico's verbonden aan onbevoegde aanwezigheid:

- Diefstal.
- Inzage door onbevoegden in privacygevoelige gegevens (documenten of dossiers).
- Manipulatie van papieren gegevens (b.v. aanvraagformulieren).
- Manipulatie van geautomatiseerde gegevens.
- Diefstal van materiële eigendommen van medewerkers.
- Observaties (voorverkenning) waarmee criminele activiteiten kunnen worden voorbereid.

Fysieke beveiligingsmaatregelen in het kader van diefstal kunnen zoal bestaan uit:

- Begeleiding van bezoekers.
- Afwezigheid van de aanduiding van kritische ruimten; geen opslag van gevaarlijke stoffen in kritische ruimten.
- Aanwezigheid van detectiemiddelen en schadebeperkende voorzieningen in en rondom kritische ruimten.

Sabotage

Onder sabotage wordt verstaan het moedwillig verstoren van het geautomatiseerde verwerkingsproces. Het probleem is hier dat we niet te maken hebben met situaties die op een of andere manier te voorzien zijn, voortkomen uit het falen van de techniek of een gevolg zijn van fouten en ongelukken. Nee, we hebben hier te maken met kwaadwillende mensen.

Sabotage kan plaatsvinden door het eigen personeel of door onbekende individuen die alleen of in groepsverband optreden. Bescherming hiertegen is, temeer daar gemeentelijke gebouwen in principe een "open" karakter hebben, moeilijk.

Nochtans is het wenselijk geen hardware in de nabijheid van ramen te plaatsen. Bevinden computers zich op de begane grond, dan is het aan te bevelen, ter voorkoming van het ingooien van ruiten, de ramen te voorzien van slagvast glas.

Virussen

Een bijzondere vorm van sabotage vormen de virussen. De grootste bedreiging voor PC's is dat deze via Internet onverhoeds een computervirus oplopen. Internet kent een groot aantal verschillende virussen. Zo zijn er de zogenaamde Trojaanse paarden: besmette programma's die verstopt zitten in andere programma's. De meeste virussen tasten de gegevens op de harde schijf aan, zodat belangrijke informatie verloren gaat, maar er zijn ook virussen die gehele PC's in een keer ruïneren.

Over het algemeen verspreiden computervirussen zich als bijgevoegde bestanden bij e-mail en via programma's die van Internet zijn te downloaden. Virussen zitten verstopt in besmette computerprogramma's die heel gewoon lijken, bijvoorbeeld een screensaver of een spelletje. Zodra u een programma opent dat besmet is met een virus, wordt dit virus actief en kan het veel schade berokkenen. Uw computer kan geïnfecteerd raken met een virus via valse bestanden of via onbetrouwbare webpagina's.

De beste verdediging tegen virussen en Trojaanse paarden is het gebruik van een recent anti-virusprogramma. Het is hierbij erg belangrijk dat er regelmatig een recente viruslijst wordt gedownload van de webpagina van de leverancier Sophos van de anti-virussoftware Sophos anti-virus.

Verder is het van groot belang dat er geen onbekende bestanden worden geopend of gedownload. Dit geldt ook voor beveiligingssoftware die u kunt downloaden van Internet. U zult helaas niet de eerste zijn die denkt een goede beveiliging aan te leggen, maar in werkelijkheid beveiligingssoftware installeert die zelf besmet blijkt te zijn met een virus of een Trojaans paard.

Fraude door derden

Door fraude kunnen criminelen reisdocumenten en/of rijbewijzen op een valse naam verwerven. Ook kan door fraude diefstal worden gemaskeerd. In de praktijk worden verschillende fraudevormen onderscheiden:

Fraude zonder medewerking (misleiding)

Hierbij proberen kwaadwillenden een document te verkrijgen op een valse naam door medewerkers te misleiden. Er wordt onderscheid gemaakt tussen *aanvraag op oneigenlijke gronden* en aanvragers die zich voordoen als een ander (*look-alike*).
Bij een aanvraag op oneigenlijke gronden maakt een (illegale) persoon bij de aanvraag van een nieuw document gebruik van de personalia van een persoon die is ingeschreven in de GBA. Indien deze aanvraag wordt toegekend, wordt een document afgegeven waarvan de foto niet overeenkomt met de personalia in het document. Bij een dergelijke fraudepoging zal de aanvrager (fraudeur) over het algemeen het oude document niet overleggen, maar gebruik maken van een ten onrechte opgemaakt proces-verbaal.
Look-alikes presenteren zich meestal bij grenscontroles, inschrijvingen bij uitzendbureaus, aanvragen van sociale uitkeringen en dergelijke. Maar ook op gemeentehuizen proberen look-alikes soms onder overlegging van een document van een ander een nieuw reisdocument te verwerven. De look-alike probeert een nieuw document te verwerven door zich voor te doen als degene van wie hij een correct afgegeven oud document bezit. De aanvrager lijkt sterk op de foto in dit oude document. Het document dat de fraudeur gebruikt, is dikwijls een vermist document dat in het criminele circuit is terechtgekomen of dat door de houder aan de fraudeur ter beschikking is gesteld.

Fraude onder druk

Hierbij proberen kwaadwillenden een document te verkrijgen op een valse naam door met chantage, bedreiging of omkoping de medewerking van medewerkers af te dwingen.

Interne fraude

Hierbij plegen medewerkers op eigen initiatief onrechtmatige handelingen of werken zij daaraan mee.

2.3.6 Onbevoegd gebruik door derden

Onbevoegd gebruik van computersystemen kan zich in velerlei vormen voordoen, van computerspelletjes tot zelfs privé-administraties toe. Omdat in de gemeentelijke organisatie de hardware decentraal is opgesteld, is onbevoegd gebruik moeilijk te constateren.

Het onbevoegd gebruik van de hardware door onbekende individuen of personeel van andere afdelingen moet in eerste instantie door fysieke beveiliging worden voorkomen. In tweede instantie kan gebruik gemaakt worden van beveiligingssoftware. Door aan het informatiesysteem kenbaar te maken welke gebruikers toegang hebben tot het informatiesysteem en welke bevoegdheden deze gebruikers hebben, wordt een drempel gelegd voor potentiële fraudeurs.

Het principe van de meeste beveiligingssoftware berust op een autorisatiematrix. Daarin is vastgelegd welke objecten beveiligd moeten zijn tegen welke handelingen van welke gebruikers. De veiligste methode is "niets toestaan tenzij uitdrukkelijk anders is bepaald". Alle handelingen van de gebruikers kunnen dan worden getoetst op rechtmatigheid.

Om toegang te krijgen tot een informatiesysteem moet de gebruiker zich identificeren met een gebruikersidentificatie en een wachtwoord. Deze combinatie - die binnen een systeem uniek is - wordt getoetst aan de autorisatiematrix. Komt deze combinatie niet in de matrix voor, dan krijgt de gebruiker geen toegang tot het systeem. Zijn poging op het informatiesysteem binnen te komen wordt geregistreerd in het logboek en geeft de applicatiebeheerder ICT de gelegenheid een passende actie te nemen, bijvoorbeeld een verscherpte controle op het gebruik van het betreffende werkstation of het veranderen van identificatie en wachtwoord.

Heeft de geautoriseerde gebruiker eenmaal toegang tot het systeem verkregen, dan zal hij gebruik willen maken van software en data. Het zal duidelijk zijn dat, naast de software, ook de in het systeem opgeslagen data beveiligd moet zijn tegen een onbevoegd gebruik (lezen, wijzigen of afdrukken). Ook dit kan in de autorisatiematrix worden opgenomen.

Opgemerkt wordt nog dat geen garantie kan worden gegeven voor een sluitende beveiliging. Een goede beveiliging is grotendeels afhankelijk van de discipline van de gebruikers en de controle daarop. Er moet zorgvuldig worden omgegaan met het gebruik van de autorisatiegegevens. Het laten slingeren van deze gegevens is te vergelijken met een huis dat wordt afgesloten en waarvan de sleutel naast het deurslot wordt gehangen.

2.3.7 Fraude door eigen personeel

De gegevensverwerking bij de gemeente Haarlem vindt vrijwel geheel plaats via computersystemen. Dit impliceert dat functies die rechtstreeks verband houden met geautomatiseerde gegevensverwerking, zoals die van de applicatiebeheerder ICT en de applicatiebeheerders, steeds meer het karakter krijgen van vertrouwensfuncties.

Daar komt nog bij dat systeem- en applicatiebeheer, gezien het specialistische karakter, moeilijk aan toezicht te onderwerpen is, zowel voor wat betreft de technische juistheid van de uitvoering als de rechtmatigheid van de verrichte handelingen.

Uit het oogpunt van beschikbaarheid mag het systeembeheer en het applicatiebeheer niet exclusief worden opgedragen aan één persoon. Onverhoopt vertrek van de applicatiebeheerder ICT - en daarmee het vertrek van alle kennis van het betreffende informatiesysteem - kan ernstige beschikbaarheidproblemen opleveren. Daarom is het aan te bevelen minimaal één plaatsvervanger aan te

wijzen en die van tijd tot tijd de systeembeheerstaak te laten vervullen. Hetzelfde geldt uiteraard voor de applicatiebeheerders.

De ervaringen hebben aangetoond dat de grootste potentiële dreiging van een informatiesysteem schuilt in het personeel dat daarvan gebruik maakt.

Daarom is een nauwkeurige selectie van personeel dat uitvoeringsverantwoordelijkheid gaat dragen voor computersystemen een aanbeveling. Daarbij moet vooral worden gelet op eigenschappen als verantwoordelijkheidsgevoel, discipline en integriteit. Hierbij kunnen een antecedentenonderzoek, diplomacontrole en natrekken van de opgegeven referenties een rol spelen.

Het is uitermate gewenst dat de arbeidsomstandigheden van automatiseringspersoneel zodanig zijn dat de beschikbaarheid van het informatiesysteem en het beheer daarvan maximaal is gewaarborgd.

Functiescheiding

Functiescheiding heeft betrekking op maatregelen die misbruik of oneigenlijk gebruik van bevoegdheden moeten voorkomen. Functiescheiding moet het mogelijk maken om (direct of achteraf) te controleren of de betrokken medewerkers hebben gehandeld zoals is voorgeschreven. De nadruk ligt op het voorkómen van fraude door externen of door interne medewerkers, al dan niet onder druk van kwaadwillenden (chantage, bedreiging of omkoping).

In de praktijk overtreft het aantal te scheiden taken vrijwel altijd het aantal medewerkers. Van een 1-op-1 functiescheiding zal daarom zelden sprake zijn. Optimale functiescheiding wordt verkregen door het zoveel mogelijk verdelen van de taken over de beschikbare medewerkers. Zie voor de concrete effectuering van de functiescheiding Bijlage Functieverdeling.

3 Informatiebeveiligingsbeleid

3.1 Beleidsdoelstelling

Beleid wordt gedefinieerd als een min of meer weloverwogen streven om bepaalde doeleinden met bepaalde middelen binnen een bepaalde tijdsvolgorde te bereiken.

Het college van B&W van de gemeente Haarlem stelt zich ten aanzien van de informatiebeveiliging als doelstelling die beveiligingsmaatregelen te treffen die enerzijds uit de wettelijke verplichtingen voortvloeien en anderzijds de beschikbaarheid, data integriteit, vertrouwelijkheid en controleerbaarheid van de gemeentelijke bedrijfsprocessen zoveel mogelijk garanderen. Deze doelstelling geldt ten aanzien van alle gegevensverwerkende processen waarvoor het college van B&W van de gemeente Haarlem de uiteindelijke verantwoordelijkheid draagt.

3.2 Wettelijke verplichtingen

Ten aanzien van de beveiliging van persoonsgegevens geldt artikel 13 van de Wet bescherming persoonsgegevens (WBP) als grondslag voor het informatiebeveiligingsbeleid. De tekst van dit artikel luidt:

> *De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*

Het College bescherming persoonsgegevens (CBP) kan de verantwoordelijke, in casu het college van B&W, aanspreken op het niveau van de maatregelen voor de beveiliging van de verwerking van persoonsgegevens en de wijze waarop het stelsel van maatregelen is geïmplementeerd en wordt nageleefd.

3.2.1 Fysieke beveiliging

Volgens de Inleiding EDP-auditing [1] moet het beveiligingsbeleid ten aanzien van de fysieke beveiliging in ieder geval de volgende onderdelen bevatten:

1. Doel van de beveiliging uitgaande van de bestaande organisatie voor de nabije toekomst.
2. Objecten die beveiligd zouden moeten worden.
3. Richtlijnen voor de wijze waarop beveiliging van de relevante objecten kan worden gerealiseerd.

Ad 1) In de doelstelling moet worden aangegeven op welke termijn het beleid moet zijn uitgevoerd en tegen welke bedreigingen beveiliging noodzakelijk is. In dit deel van het Informatiebeveiligingsplan is in hoofdstuk 2 aangegeven tegen welke bedreigingen er beveiligd moet worden. In hoofdstuk 4 is per risicogroep concreet aangegeven welke beveiligingsmaatregelen zijn c.q. zouden moeten worden getroffen.

Ad 2) Waar gegevens bij uitstek het beveiligingsobject zijn van het informatiebeveiligingsbeleid, zijn het gebouw, het personeel en de werkplek de beveiligingsobjecten van het fysieke beveiligingsbeleid.

[1] Zie Jan van Praat & Hans Suerink, Inleiding EDP-auditing, Kluwer Bedrijfsinformatie Deventer, januari 2001, ISBN 90 440 0199 X.

Ad 3) De richtlijnen voor het fysiek beveiligen van de objecten zijn door de gemeente Haarlem gedetailleerd in de Maatregelenanalyse van de risicoanalyse beschreven.

3.2.2 Informatiebeveiliging

Informatiebeveiligingsbeleid is volgens de Code voor Informatiebeveiliging [2] het op schrift gesteld en door het gemeentebestuur en de directie goedgekeurde beveiligingsbeleid met betrekking tot de informatievoorziening met hierin een formulering van de volgende elementen:

1. Een definitie van de term "informatiebeveiliging".
2. Een beschrijving van de belangrijkheid van informatiebeveiliging ten aanzien van het primaire proces.
3. Een verklaring over de betrokkenheid van de directie met betrekking tot informatiebeveiliging.
4. Een beschrijving van de algemene en specifieke verantwoordelijkheden voor alle aspecten van informatiebeveiliging binnen de organisatie.
5. Een bepaling over de frequentie, waarmee dit document opnieuw beoordeeld moet worden.
6. Uitspraken over confirmatie aan de door de wetgever gestelde eisen.

Ad 1) Onder informatiebeveiliging wordt in dit kader verstaan een samenhangend geheel van maatregelen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens garandeert en de controleerbaarheid van de getroffen maatregelen. Als beleidsdoelstelling wordt de eis neergelegd dat de informatiesystemen aangeduid in voorliggend plan een beschikbaarheid tijdens werktijd kennen van minimaal 95%. Buiten werktijd worden er geen eisen gesteld aan de beschikbaarheid met uitzondering van voorzieningen in het kader van rampenbestrijding.

Ad 2) De gemeentelijke bedrijfsvoering komt onmiddellijk in problemen wanneer er inbreuken worden gedaan op de informatiebeveiliging. Dat betekent dat het primaire proces slechts mogelijk is wanneer het niveau van informatiebeveiliging op een voldoende hoog niveau wordt gelegd. Bedreigingen kunnen we nimmer wegnemen. De kans op het manifest kan echter kleiner worden gemaakt door het treffen van preventieve maatregelen. De (gevolg)schade die wordt geleden kan worden beperkt door repressieve- en herstelmaatregelen.

Ad 3) Zie het vervolg van dit hoofdstuk voor een verklaring over de betrokkenheid van het gemeentebestuur en de directie met betrekking tot informatiebeveiliging.

Ad 4) Zie het vervolg van dit hoofdstuk voor uitspraken over de verantwoordelijkheden zoals de directie die ziet.

Ad 5) Dit document wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de beveiligingsbeheerder en bij noodzaak daartoe bijgesteld. Alle medewerkers van de gemeente worden via de gebruikelijke interne kanalen en voor zover noodzakelijk door hun leidinggevende via het reguliere werkoverleg geïnformeerd over voor hen van belang zijnde wijzigingen in beveiligingsbeleid, -plan, -maatregelen en/of –procedures.
Alle wijzigingen die direct betrekking hebben op individuele taken en bevoegdheden worden expliciet door de leidinggevende met zijn of haar betrokken medewerker(s) rechtstreeks gecommuniceerd.

Ad 6) De gemeente Haarlem zal zich houden aan de bepalingen van de in het kader van informatiebeveiliging relevante wet- en regelgeving zoals het Wetboek van Strafrecht, het Wetboek van Strafvordering (Wet computercriminaliteit), alsmede de relevante regelgeving.

[2] Zie de Code voor Informatiebeveiliging 2000, Een leidraad voor beleid en implementatie, Nederlands Normalisatie Instituut te Delft 2000, ICS 35.020, SPE norm 20003.

Beveiliging is geen doel op zich, maar een middel. De kosten moeten opwegen tegen de baten. De baten zijn echter moeilijk meetbaar. Het beveiligingsbeleid zal nauw moeten aansluiten op de cultuur van de gemeentelijke organisatie, de eigen bedrijfsprocessen en de binnen de organisatie gehanteerde terminologie. Dit alles zal de acceptatie van het beveiligingsbeleid sterk verhogen.

3.2.3 Raakvlakken met ander beleid

Het informatiebeveiligingsbeleid heeft raakvlakken met het beleid en de daaruit voortvloeiende procedures die zijn gericht op de operationele veiligheid van het uitgifte en beheerproces van waardedocumenten.

Informatiebeveiligingsbeleid maakt deel uit van het totale beveiligingsbeleid van de gemeente. Binnen dit beleidsterrein kan er onderscheid worden gemaakt tussen fysieke toegangsbeveiliging, identificatie van gebruikers (logische toegangsbeveiliging), sleutelbeleid, personeelsbeleid en een clean desk policy.

3.3 Taken, verantwoordelijkheden en bevoegdheden

De verantwoordelijkheid voor het Informatiebeveiligingsplan ligt te allen tijde bij de verantwoordelijke (= het college van B&W).
Deze stelt het Informatiebeveiligingsplan op en ziet toe op de uitvoering ervan door de betreffende medewerkers.
De beveiligingsbeheerder is verantwoordelijk voor de voor het toezicht op de naleving van de beveiligings-maatregelen en –procedures van het Informatiebeveiligingsplan en ziet erop toe dat eens per jaar gecontroleerd wordt of de nog te nemen maatregelen gerealiseerd zijn en dat het Informatiebeveiligingsplan hierop aangepast wordt.

Voor alle in dit informatiebeveiligingsplan voorkomende functies is in Bijlage Functieverdeling de vervanging vastgelegd.

3.3.1 Verantwoordelijkheden gemeentebestuur

Beveiliging is op bestuurlijk niveau de verantwoordelijkheid van het college van B&W van de gemeente Haarlem. Het college van B&W stelt dit Informatiebeveiligingsplan vast.

Het college van B&W onderschrijft volledig de beveiligingsmaatregelen die in dit Informatiebeveiligingsplan worden voorgeschreven en wenst dat de stand van zaken met betrekking tot de informatiebeveiliging jaarlijks wordt geëvalueerd om er voor zorg te dragen dat de informatiebeveiliging in de gemeente up-to-date blijft.

Voor alle gegevensverwerkende processen rond het beheer en uitgifte van waardedocumenten heeft de burgemeester op basis van de Paspoortwet en het Reglement rijbewijzen de uiteindelijke verantwoordelijkheid.

Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van onderhavig Informatiebeveiligingsplan is de functie van beveiligingsbeheerder in het leven geroepen. Deze heeft de verantwoordelijkheid toe te zien op naleving van de beveiligingsmaatregelen en –procedures zoals uitgewerkt in voorliggend Informatiebeveiligingsplan en daarover aan het college van B&W te rapporteren.

De functie van de beveiligingsbeheerder moet niet verward worden met de functie van ‘de beveiligingsfunctionaris reisdocumenten’ noch die van ‘de beveiligingsfunctionaris rijbewijzen’. Beide laatstgenoemde functies kennen zeer specifieke taken en verantwoordelijkheden op het beveiligingsgebied van enerzijds de reisdocumenten en anderzijds de rijbewijzen. De inhoud van beide functies zal apart worden toegelicht.

3.3.2 Verantwoordelijkheden van de directie

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle leden van de directie van de gemeente Haarlem.

De directie bepaalt binnen de gegeven bestuurlijke kaders de koers van het ambtelijk apparaat.

Per jaar zullen de volgende punten met betrekking tot beveiliging aan de orde komen:

- Voortgang realisatie beveiligingsmaatregelen als beschreven in het Informatiebeveiligingsplan en gerapporteerd door de beveiligingsbeheerder.
- Mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen.
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingsbeheerder
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingsfunctionaris reisdocumenten en/of de beveiligingsfunctionaris rijbewijzen.
- Goedkeuring van initiatieven om de (informatie)beveiliging te verbeteren.
- Geven van voor een ieder zichtbare ondersteuning bij de implementatie van beveiligingsmaatregelen.
- Bevorderen van het beveiligingsbewustzijn.
- Herziening en goedkeuring beveiligingsbeleid en de toegekende verantwoordelijkheden.

3.3.3 Verantwoordelijkheden van de beveiligingsbeheerder

Door het college van B&W is de beveiligingsbeheerder benoemd. De beveiligingsbeheerder is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Informatiebeveiligingsplan. De beveiligingsbeheerder rapporteert periodiek (minimaal eens per jaar) aan het college van B&W en de directie, zo nodig zonder tussenkomst van de diverse afdelingsmanagers.

Onder beveiligingsbeheerder wordt verstaan: een medewerker die kennis en ervaring heeft op het gebied van informatiebeveiliging en op dit terrein een adviserende en coördinerende rol kan vervullen.

De beveiligingsbeheerder is verantwoordelijk voor:

- Toezicht op de voorbereiding, implementatie en uitvoering van het beveiligingsbeleid en –plan.
- Een jaarlijkse rapportage over de voorbereiding, implementatie en uitvoering van het beveiligingsbeleid en –plan aan het college van B&W en de directie.
- Rapportage van beveiligingsincidenten.
- Het toezicht op de naleving van de beveiligingsprocedures.
- Toezicht houden op het feit dat minstens eenmaal per jaar voorlichting of instructie aan medewerkers wordt verzorgd, door middel van toetsing van de opgestelde beveiligingsprocedures in de praktijk.
- Toezicht houden op het feit dat nieuwe medewerkers worden geïntroduceerd en bekend gemaakt met de beveiligingsprocedures.

De beveiligingsbeheerder verstrekt daarnaast gevraagd en ongevraagd adviezen om te komen tot het gewenste beveiligingsniveau.

3.4 Passende technische en organisatorische maatregelen

Welk niveau van technische en organisatorische maatregelen passend is wordt bepaald door de risicoklasse, waarin de persoonsgegevens worden ingedeeld.
De in de GBA vastgelegde persoonsgegevens zijn op grond van de door het College bescherming persoonsgegevens (CBP) gehanteerde classificatie ingedeeld in risicoklasse II (verhoogd risico), dat wil zeggen er bestaan in vergelijking met het basisniveau van risicoklasse I extra negatieve gevolgen voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De indeling in deze risicoklasse komt voort uit de aard van de gegevensverwerking in de GBA: de gegevens die worden verwerkt hebben betrekking op de gehele bevolking van de gemeente Haarlem.

Een passend beveiligingsniveau
Een adequaat niveau van beveiliging van persoonsgegevens kan worden bereikt door het treffen van een stelsel van technische en organisatorische maatregelen, waarvan het niveau aansluit bij de risico's die verbonden zijn aan de gedefinieerde risicoklasse.

De te nemen maatregelen worden gewogen aan de hand van de volgende criteria:
- Stand van de techniek.
- Kosten.
- Risico's zowel van de verwerking, als ook van de aard en de omvang van de persoonsgegevens.

3.4.1 Kwaliteitsaspecten

Informatiebeveiligingsbeleid is niets anders dan een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijk top eendrachtig duidelijk maken aan het tactisch en operationeel niveau welke gedragslijn de gemeente Haarlem dient te volgen om te komen tot een adequate informatiebeveiliging. Het beleid vormt daarmee de basis voor de hieronder uitgewerkte normen en maatregelen.
Het maken en vaststellen van beveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten in een informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het management vast te stellen of de maatregelen werken. Evaluatie van het beleid dient vervolgens plaats te vinden om na te gaan of het beleid nog steeds aansluit op de organisatie en of de juiste maatregelen zijn getroffen.

De beveiliging van persoonsgegevens kent drie kwaliteitsaspecten, namelijk:

1e: **beschikbaarheid** De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften. Beschikbaarheid wordt gedefinieerd als de ongestoorde voortgang van een gegevensverwerking.

2e: **integriteit** De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.

3e: **vertrouwelijkheid** Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.

Een vierde aspect dat hierbij een rol speelt is controllability. Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, Assurance, audit trail) van groot belang. Controleerbaarheid is de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd.

De gemeente Haarlem hanteert voor deze kwaliteitsaspecten de volgende normen:

3.4.1.1 Norm voor beschikbaarheid

Het College van B&W en de directie zijn van mening dat de bedrijfsvoering geheel stil komt te liggen als de informatievoorziening voor wat betreft een aantal kritische applicaties wordt gestaakt. Dit geldt onder andere voor de GBA applicatie.
De informatievoorziening rondom Probev moet tijdens de **openingstijden** van het gemeentehuis, op jaarbasis gemiddeld voor **98%** beschikbaar zijn.

De openingstijden (voor het publiek) zijn:

Maandag tot en met woensdag en vrijdag van 9.00 - 16.00 uur; donderdag van 9.00 tot 20.00 uur.

Daarnaast dient de informatievoorziening rondom Probev op jaarbasis tijdens **kantooruren** voor **97%** beschikbaar te zijn.

Als kantooruren worden hier bedoeld:

Maandag tot en met woensdag en vrijdag 9.00 uur - 16.00 uur; donderdag van 09.00 tot 20.00 uur.

Een uitval mag echter nooit langer duren dan 48 uur. Er dienen voldoende adequate voorzieningen te zijn getroffen om zelfs in geval van calamiteiten na **maximaal 48 uur** de dienstverlening aan de burger en aan andere bestuursorganen (waaronder de landelijke afnemers en andere gemeenten die zijn aangesloten op het landelijk GBA-netwerk) te kunnen voortzetten.

3.4.1.2 Norm voor integriteit

De technische en organisatorische inrichting van de gemeentelijke informatiesystemen zijn zodanig van aard en opzet dat de gegevens daarin volledig zijn opgenomen, juist en actueel zijn. De verantwoordelijke personen en afdelingen van de gemeentelijke organisatie treffen hiervoor de nodige maatregelen.

3.4.1.3 Norm voor vertrouwelijkheid

Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van in de diverse registraties opgenomen gegevens. De bevoegdheid van een persoon moet worden afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon, dit ter beoordeling van de informatiebeheerder, op aangeven van de direct leidinggevende van de betreffende medewerker. Alle medewerkers die met GBA gegevens in aanraking komen dienen een geheimhoudingsverklaring te hebben ondertekend.

Alle meldingen van verwerkingen van persoonsgegevens die in de zin van de Wet gemeentelijke basisadministratie persoonsgegevens en de Wet bescherming persoonsgegevens verplicht zijn, zijn door de gemeente gedaan aan het College bescherming persoonsgegevens in Den Haag.

3.4.1.4 Norm voor controleerbaarheid

Mutaties in persoonsgegevens kunnen verstrekkende gevolgen hebben die ver buiten het domein van de gemeente Haarlem uitgaan. Rechtstreekse toelating tot Nederland is afhankelijk van de nationaliteit. Hoogte en duur van uitkeringen zijn rechtstreeks afhankelijk van leeftijd en burgerlijke staat. De gemeente Haarlem kent dan ook als norm dat 99% van alle mutaties in persoonsgegevens herleidbaar moet zijn tot een individuele medewerker die hiervoor verantwoordelijk is, en dat zulks geldt voor 90% van alle raadplegingen. Met de implementatie van "Proweb" in het najaar van 2009, zal ook aan de hier laatst genoemde vereiste voldaan zijn.

3.4.1.5 Samenvatting

Beveiliging van (persoons)gegevens vraagt om een zorgvuldige analyse van de risico's die met de gegevensverwerking samenhangen. Er kunnen verschillende risico's worden genoemd die ertoe kunnen leiden dat het verwerkingsproces stagneert, zoals verlies van gegevens (raakt aan de kwaliteitsaspecten integriteit en beschikbaarheid) en onrechtmatig gebruik van gegevens (raakt aan het aspect vertrouwelijkheid). De in het voorliggend Informatiebeveiligingsplan opgenomen procedures dekken de risico's, behorend bij de aan de verwerking van persoonsgegevens verbonden risicoklasse (II) af.

4 Risicoanalyse

4.1 Inleiding

Het optreden van een gebeurtenis die, bij het ontbreken van passende maatregelen, duidelijk waarneembare gevolgen (materieel dan wel immaterieel) voor de organisatie heeft, noemen we een calamiteit. Het benoemen van deze calamiteiten is niet altijd noodzakelijk. In veel gevallen is het definiëren van specifieke calamiteiten die een gemeente zouden kunnen treffen zelfs een barrière: het heeft het gevaar in zich dat de beschikbaarheidvoorziening te beperkt opgezet wordt.

Hoewel voor elke organisatie verschillend, is het toch mogelijk een aantal gevolgen van een calamiteit te noemen:

- Vitale informatie gaat verloren.
- Financiële controle is niet meer mogelijk.
- Informatie is niet meer beschikbaar.
- Goederen en diensten kunnen niet geleverd worden.
- Demotivatie bij medewerkers.
- Chaos.
- Fraude.

4.2 Het hoe en waarom van een risicoanalyse

Voordat de uitgangspunten waaraan de informatiebeveiliging moet voldoen bepaald worden, wordt een risicoanalyse inclusief een gevolgschade onderzoek uitgevoerd om de risico's voor de bedrijfsprocessen te analyseren. Later kunnen dan voor de kritieke bedrijfsprocessen de juiste risico's weggenomen of tot een acceptabel niveau worden beperkt. Wordt deze analyse overgeslagen dan worden maatregelen gekozen die wellicht het beoogde doel niet waarborgen.

Een *risicoanalyse* kan op een aantal manieren plaatsvinden; een veel gebruikte manier is de kwantitatieve methode waarbij de risico's voor het manifest worden van alle onderkende bedreigingen (het optreden van een calamiteit dus) voor de organisatie bepaald worden.

Bij een *gevolgschade onderzoek* (die aan de hand van de risicoanalyse uitgevoerd kan worden) wordt de materiële (en wellicht ook de immateriële) schade die optreedt bij het manifest van een calamiteit per gebeurtenis gekwantificeerd en daarna gesommeerd. De totale schadeverwachting per jaar geeft de directie gereedschap in handen om de kosten van voorzieningen te relateren aan de te vermijden risico's.

In de laatste jaren komt de kwalitatieve methode meer in zwang. Hierbij worden risico's niet meer in cijfers achter de komma bepaald maar worden klassen samengesteld en kan de directie vervolgens keuzen maken welke risico's men wil kunnen overleven.
Deze methode levert meer 'tastbare' handvatten. De directie ziet hierdoor in een oogopslag welke processen de hoogste prioriteit dienen te krijgen. De kwalitatieve methode wordt in het voorliggend Informatiebeveiligingsplan toegepast.

4.3 Waarschijnlijkheid en effect

Om de beveiliging verder te verbeteren, moet een risicoanalyse worden uitgevoerd. In hoofdstuk 2 is al geconstateerd dat er bedreigingen zijn voor de informatiebeveiliging van het GBA en voor de reisdocumenten en rijbewijzen;

Er wordt een zevental bedreigingen onderscheiden bij het GBA:

1. Bliksem, brand en explosie.
2. Stof, vuil en water.
3. Stroomuitval, storingen en fouten.
4. Diefstal, sabotage, virussen en fraude door derden.
5. Onbevoegd gebruik.
6. Beschikbaarheid.
7. Personeel.

Er wordt een negental bedreigingen onderscheiden bij het BeveiligingsNet:

1. Taken, verantwoordelijkheden en bevoegdheden.
2. Beveiligingsbeleid, beveiligingsplan, communicatie en onderzoek.
3. Organisatorische maatregelen en autorisaties.
4. Bouwkundige en elektronische voorzieningen.
5. ICT beveiliging.
6. Identiteitsverificatie.
7. Beslissing op de aanvraag.
8. Ontvangst, uitreiken en onttrekking reisdocumenten.
9. Beheer en administratie van reisdocumenten, formulieren en materialen.

Niet al deze bedreigingen zijn even groot. Om toch een inschatting te maken van de ernst van de risico's worden twee factoren ingevoerd waarmee de risico's ten opzichte van elkaar kunnen worden gewogen: **waarschijnlijkheid** en **effect**.

Waarschijnlijkheid
Het begrip waarschijnlijkheid heeft betrekking op de kans dat een incident zich zal voordoen. Deze inschatting is moeilijk te maken. Niet alles over wat zich aan ongewenste incidenten voordoet, is bekend. In de risicoanalyse is expertkennis gekoppeld aan interviews met betrokkenen bij de gemeente Haarlem. De bevindingen hiervan hebben geleid tot vooral de beveiligingsmaatregelen zoals opgesomd in de volgende paragraaf van dit Informatiebeveiligingsplan.

Effect
De schade van genoemde incidenten kan aanzienlijk zijn. Niet alleen omdat waardevolle documenten of informatie verloren kunnen c.q. kan gaan, maar ook omdat de gevolgen voor medewerkers groot kunnen zijn. Ook kan het incident nadelige gevolgen hebben voor het beeld van de gemeente (en van de hoofdafdeling Dienstverlening in het bijzonder) bij het publiek.

4.4 Prioriteitstelling

De risico's zijn in de risicoanalyse ten opzichte van elkaar gewogen op de aspecten "waarschijnlijkheid" en "effect". Uit de combinatie van "waarschijnlijkheid" en "effect" kan de grootte van het risico worden bepaald. Dit leidt vervolgens tot een zogenoemde prioriteitstelling: een volgorde van de risico's waar men zich tegen moet wapenen.

WAARSCHIJNLIJKHEID	**EFFECT**
Vier niveaus van waarschijnlijkheid	*Vier niveaus van gevolgschade*
1. ONBEDUIDEND ▪ geen geregistreerde of aantoonbare incidenten; ▪ geen recente incidenten.	**1. ONBEDUIDEND** ▪ geen meetbaar effect; ▪ te verwaarlozen invloed op imago bij het publiek.
2. LAAG ▪ zeer weinig geregistreerde incidenten; ▪ wel vermoeden maar geen aantoonbare incidenten.	**2. GERING** ▪ er zijn aantoonbare kosten op lokaal niveau, niet op centraal niveau; ▪ implicatie voor imago bij het publiek op lokaal niveau.
3. GEMIDDELD ▪ regelmatig geregistreerde incidenten of een zichtbare trend; ▪ sterke aanwijzing uit meerdere bronnen.	**3. BEDUIDEND** ▪ kan een merkbaar gevolg hebben op de bedrijfsvoering; ▪ serieuze schade aan het imago bij het publiek met aanmerkelijke kosten voor herstel.
4. HOOG ▪ aantal incidenten wijst op een kritieke situatie of een campagne tegen de gemeente; ▪ grote waarschijnlijkheid van toekomstige incidenten gebaseerd op geïdentificeerde factoren.	**4. KRITIEK** ▪ ernstige ontwrichting van de bedrijfsvoering; ▪ bedrijfsvoering op lange termijn wordt aangetast; ▪ ernstige aantasting van het imago van de gemeente bij het publiek met hoge kosten en grote inspanning voor herstel.

Figuur 1 Verduidelijking prioriteitsstelling

Het informatiebeveiligingsbeleid van de gemeente Haarlem stelt dat de beschikbaarheid van de gegevensprocessen zoveel mogelijk moet zijn gegarandeerd. In dit kader zijn technische en organisatorische maatregelen noodzakelijk om een passend beveiligingsniveau te bereiken.
Deze maatregelen moeten zijn gebaseerd op een zorgvuldige risicoanalyse, waarbij de lokale fysieke omstandigheden bepalend zijn voor de omvang van de bedreigingen. Teneinde deze risico's te inventariseren en adequate voorzieningen te treffen om de beschikbaarheid van de gegevensprocessen te garanderen is een risicoanalyse uitgevoerd met de leden van de overleggroep Informatiebeveiliging GBA en waardedocumenten van de gemeente Haarlem.

Met de overleggroep Informatiebeveiliging GBA en waardedocumenten is op 12 december 2008 een afweging gemaakt van de kans op het optreden van deze bedreigingen en het effect van de bedreiging op de beschikbaarheid van de gegevensverwerking. Het product van de kans op het optreden van de bedreiging maal het effect op de beschikbaarheid van de gegevensverwerking heeft geleid tot een prioriteitsstelling in de genoemde risico's. Het resultaat hiervan is zichtbaar gemaakt in de volgende tabel.

Bedreiging	**Waarschijnlijkheid**	**Effect**	**Prioriteit** *)
Brand	1	3	3
Explosie	1	3	3
Bliksem	1	3	3
Stof, vuil en water	1	2	2
Klimaat beheersing	1	4	4
Stroomstoring	2	4	8
Hardware storingen	1	4	4
Software storingen	2	4	8
Lekkage	1	2	2
Inbraak	1	3	3
Diefstal	2	3	6
Overval	1	4	4
Sabotage	1	4	4
Virussen	1	3	3
Hacking	1	4	4
Externe fraude	2	4	8
Interne fraude	2	3	6
Fraude onder druk	2	3	6
Uitlekken gevoelige informatie	2	2	4
Ongeautoriseerd gebruik systeem	3	3	9
Back-up voorzieningen	1	4	4
Beschikbaarheidvoorzieningen	1	3	3
Fysiek geweld	1	4	4
Verbaal geweld	1	4	4
Kwalitatieve onderbezetting	1	3	3
Kwantitatieve onderbezetting	2	3	6
Attitude personeel	1	3	3
Vandalisme	1	4	4
Onbevoegde aanwezigheid	1	1	1
Vermissing waardedocumenten	1	4	4

*) prioriteit 1 = hoogste prioriteit *(waarschijnlijkheid x effect)*

Figuur 2 Risico en prioriteitsstelling

Toelichting op deze bevindingen:

Voor een groot aantal bevindingen geldt dat de waarschijnlijkheid en soms mede daardoor het effect in deze voor de gemeente Haarlem onbeduidend tot gering is. Alle risico's zijn met een gemiddelde score uit de risicoanalyse gekomen. Stroomstoring, software storingen, externe fraude en ongeautoriseerd gebruik van het systeem zijn met een relatief hoge prioriteitswaarde uit de risicoanalyse gekomen, waardoor aandacht voor deze risico's gewenst is. Dit betekent dat deze risico's met voorrang dienen te worden beoordeeld bij het bepalen van de te nemen beveiligingsmaatregelen. De acties die hierop ondernomen moeten worden zijn opgenomen in de maatregelen analyse, die onderdeel is van dit beveiligingsplan.

Procedures beveiligingsplan algemeen
Procedure Afvoeren van computers
Procedure Antivirus voorzieningen
Procedure Autorisatie tot het systeem
Procedure Back-up van de GBA applicatie
Procedure Communicatie over beveiliging
Procedure Goedkeuren updates applicatie
Procedure Identificatie en Machtiging
Procedure Kasbeheer
Procedure Overvalinstructie en agressief publiek
Procedure Rapportage van incidenten
Procedure Restore van de GBA applicatie
Procedure Uitwijk
Procedure Vernietiging van verwijderbare media

Bijlagen beveiligingsplan algemeen
Bijlage Aangifteformulier overval
Bijlage Activiteitenkalender informatiebeveiliging
Bijlage Back-up registratie
Bijlage beveiligingsdocumentatiedossier
Bijlage Bewerkersovereenkomst
Bijlage Formulier Autorisaties
Bijlage Functieverdeling
Bijlage Geheimhoudingsverklaring
Bijlage Kenmerken Computerruimte
Bijlage Kenmerken fysieke beveiliging
Bijlage Kenmerken GBA applicatie
Bijlage Kenmerken GBA systeem
Bijlage Kenmerken Gemeentelijke LAN
Bijlage Machtiging BZK Bewerker
Bijlage Onderhoudscontract
Bijlage Proces verbaal vernietiging van verwijderbare media
Bijlage Uitwijkcontract
Bijlage Verklarende woordenlijst
Bijlage Vragenlijst bewerker

Rapportages beveiligingsplan algemeen
Rapportage beproeving communicatie over beveiliging
Rapportage controle autorisaties
Rapportage evaluatie beveiligingsbeleid en plan
Rapportage test reconstructie
Rapportage test restore
Rapportage test uitwijk
Rapportage test verstrekking alt medium

5 GBA en waardedocumenten

5.1 Inleiding

Het op schrift stellen van de - in praktijk van alledag al ingeburgerde – beveiligingsprocedures is noodzakelijk om objectief te kunnen bepalen of de GBA-bestanden en bepaalde processen voldoen aan de eisen ten aanzien van beschikbaarheid (continuïteit), integriteit (betrouwbaarheid), vertrouwelijkheid (exclusiviteit) en controleerbaarheid.

De gemeente moet in het kader van de **Wet bescherming persoonsgegevens** (WBP) "passende" beveiligingsmaatregelen nemen. In het begrip "passend" ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens.

Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van gegevens.

Daarnaast stelt de wetgever eisen aan de opslag, uitgifte en administratie van reisdocumenten. Deze eisen zijn neergelegd in de Paspoortuitvoeringsregeling Nederland 2001, kortweg 'PUN' genoemd. Hoofdstuk XII van deze wet met als onderwerp beveiliging begint met een algemeen artikel dat luidt: "De met de uitvoering van de wet belaste autoriteiten treffen maatregelen om de onder hen berustende reisdocumenten, bijschrijvingsstickers, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreemding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins".

Deze te treffen maatregelen worden in dit beveiligingsplan verder uitgewerkt in concrete voorschriften op het gebied van fysieke beveiliging, back-up en herstel en enkele voorschriften over hoe te handelen in bepaalde situaties. Artikel 93 lid 1 PUN vereist daartoe organisatorische maatregelen.

De bij de jaarlijkse evaluatie van het beheerproces rond waardedocumenten geconstateerde afwijkingen worden schriftelijk vastgelegd en 5 jaar bewaard. Op de eventueel geconstateerde lacunes wordt actie ondernomen.

Daarnaast is door de wetgever een jaarlijks onderzoek naar de staat van beveiliging rond de reisdocumenten verplicht gesteld. Het agentschap BPR van het Ministerie van Binnenlandse zaken heeft voor dit onderzoek een hulpmiddel ontwikkeld. Dit hulpmiddel, een uitgebreide vragenlijst in de vorm van een 'software-tool', kent de naam 'BeveiligingsNet' en is uitgangspunt voor de beveiliging van de waardedocumenten in dit Informatiebeveiligingsplan.

De uitgifte van rijbewijzen is met de komst van het nieuwe rijbewijs drastisch veranderd. Het uitgifteproces van rijbewijzen komt inmiddels sterk overeen met dat van de Nieuwe Generatie Reisdocumenten. De wetgever stelt dan ook ten aanzien van de uitgifte van rijbewijzen eveneens eisen aan de beveiliging hiervan. Zo wordt geëist dat de met afgifte van rijbewijzen belaste autoriteiten zorgdragen voor een op schrift gestelde beveiligingsprocedure, met in ieder geval beveiligingsvoorschriften ten aanzien van: toegang van personen tot en het beheer van rijbewijzen, de met de afgifte van rijbewijzen verband houdende materialen, apparatuur, toegangspassen en gebruikerscodes tot de apparatuur, de verantwoordelijkheden van de beveiligingsfunctionaris en de functiescheiding.

5.2 Periodieke audit, onderzoek en accountantscontrole

De in het voorliggend Informatiebeveiligingsplan voorgestelde beveiligingsmaatregelen en –procedures vormen voor een groot deel eens in de drie jaar object van onderzoek bij de door het ministerie van Binnenlandse Zaken en Koninkrijkrelaties, agentschap BPR, voorgeschreven GBA-audit. Hierbij wordt aangetekend dat bij de GBA-audit niet alleen wordt gekeken naar opzet en bestaan van

de maatregelen, maar ook naar de werking, wat een regelmatige beproeving van de beschreven procedures noodzakelijk maakt.
Het is niet te voorkomen dat gegevens fouten bevatten. Een foutloos bestand met GBA-gegevens is een nobel streven, maar is niet realistisch als concrete eis. Ook binnen de periodieke GBA-audit wordt een foutenmarge geaccepteerd. Als kwaliteitsnorm bij het bepalen van de kwaliteit van de GBA-gegevens wordt door de gemeente Haarlem een foutenpercentage geaccepteerd dat overeenkomt met de normstelling die bij de GBA wordt gehanteerd; te weten de gegevensklassen A, B en C met een foutenpercentage van respectievelijk maximaal 1, 5 en 10%.

De reikwijdte van dit Informatiebeveiligingsplan omvat ook de procedures en maatregelen die verplicht gesteld zijn in het kader van de Paspoortuitvoeringsregeling Nederland 2001 (PUN). De PUN is op 1 oktober 2001 in werking getreden en richt zich op de beveiliging van reisdocumenten. De procedures zullen één keer per jaar onderwerp zijn van intern onderzoek met behulp van het zogenaamde 'BeveiligingsNet'. De resultaten van deze jaarlijkse evaluatie worden gerapporteerd aan de burgemeester. Daarnaast wordt eens in de 3 jaar door een externe deskundige een controle uitgevoerd op de wijze waarop het jaarlijks onderzoek en de jaarlijkse actualisering van het Informatiebeveiligingsplan (onderdeel waardedocumenten) heeft plaatsgevonden. Van deze rapportage van de externe controle wordt een afschrift aan het agentschap BPR gestuurd. De beveiligingsfunctionaris reisdocumenten neemt kennis van zowel de resultaten van het jaarlijkse interne onderzoek als van de resultaten van de driejaarlijkse externe controle en houdt toezicht op de te ondernemen acties op geconstateerde tekortkomingen.

Ook de procedures rond het verstrekken van rijbewijzen zijn onderwerp van controle. Op grond van artikel 128 lid 7 van het Reglement rijbewijzen moeten de maatregelen zoals genoemd in artikel 128 lid 1 van dit reglement jaarlijks onderdeel uitmaken van de accountantscontrole.

5.3 Beveiliging persoonsgegevens

Naast de WBP kent de Wet GBA een aantal voorschriften ten aanzien van de beveiliging van de persoonsgegevens. Deze zijn voornamelijk terug te vinden in het Logisch Ontwerp GBA (hoofdstuk 7, Eisen ten aanzien van het beheer).

Het agentschap BPR stelt eisen ten aanzien van het beheer van persoonsgegevens in en rondom de GBA, die in een driejaarlijkse cyclus door een onafhankelijke auditinstelling worden getoetst. Daarbij worden een aantal verplichte maatregelen beoordeeld op het bestaan, de opzet en de werking ervan in de praktijk.

Verder zijn voor de inhoud van dit Informatiebeveiligingsplan ook de bepalingen vanuit de PUN 2001 van belang. De hier voorgeschreven richtlijnen en procedures zijn in dit Informatiebeveiligingsplan opgenomen.
Voor wat betreft het onderdeel Rijbewijzen zijn het de bepalingen in de artikelen 122 tot en met 130 van het Reglement Rijbewijzen die handelen over de beveiliging.

5.4 Taken, verantwoordelijkheden en bevoegdheden (onderdeel GBA en waardedocumenten).

Op grond van of krachtens de Wet GBA, de Paspoortwet en het Reglement Rijbewijzen dienen de taken, verantwoordelijkheden en bevoegdheden van een aantal functionarissen te worden toegekend en vastgelegd. Dit betreft de informatiebeheerder GBA, de gegevensbeheerder GBA, de privacybeheerder GBA, de applicatiebeheerder GBA, de systeembeheerder GBA, beveiligingsfunctionaris reisdocumenten, de Autorisatie Bevoegde Reisdocumenten, de

beveiligingsfunctionaris rijbewijzen en de Autorisatie Bevoegde Rijbewijzen. Aan deze eis wordt in dit hoofdstuk voldaan.

Voor alle in dit hoofdstuk voorkomende functies is in Bijlage Functieverdeling de vervanging vastgelegd.

5.4.1 Verantwoordelijkheden van de informatiebeheerder GBA

De manager hoofdafdeling Dienstverlening is aangewezen als informatiebeheerder van het GBA-systeem. Deze zorgt vervolgens voor het toewijzen van taken en verantwoordelijkheden om de hiervoor genoemde vertrouwelijkheid te waarborgen en te controleren.

De informatiebeheerder is manager van het betreffende organisatieonderdeel en bepaalt in het kader van de beveiliging het volgende:

- Het beleid en de keuze rondom de bedrijfsproces ondersteunende applicatie(s) ten behoeve van de GBA.
- Wie de taken de applicatiebeheerder GBA en de gegevensverwerking GBA uitvoeren.
- Het niveau van autorisatie voor de eindgebruikers voor de GBA applicatie(s).
- Het aan de medewerkers van de hoofdafdeling Dienstverlening verlenen van het recht om hun ervaringen rondom aspecten van beveiliging aan de orde te stellen.
- Het onderwerp informatiebeveiliging tenminste eenmaal per jaar te agenderen op het reguliere werkoverleg van de hoofdafdeling Dienstverlening.
- Het verplichten van medewerkers van de hoofdafdeling Dienstverlening tot het direct melden van onregelmatigheden met betrekking tot de beveiliging.
- Het aanspreken van medewerkers van de hoofdafdeling Dienstverlening op geconstateerd onzorgvuldig gedrag in relatie tot beveiliging en het zonodig voorstellen van disciplinaire maatregelen.
- Het alle medewerkers van de hoofdafdeling Dienstverlening in de gelegenheid stellen om aan relevante trainingscursussen deel te nemen, die door deskundigen wordt verzorgd, een en ander tot bevordering van de beveiligingsbewustwording.
- De gelegenheid bieden aan medewerkers van de hoofdafdeling Dienstverlening tot het volgen van cursussen, trainingen en opleidingen in het kader van informatiebeveiliging en dit bevorderen.

De informatiebeheerder GBA kan de uitvoering van hiervoor genoemde taken geheel of gedeeltelijk delegeren aan de daartoe in de Bijlage Beheerregeling GBA aangewezen medewerkers.

5.4.2 Verantwoordelijkheden van de gegevensbeheerder GBA

De gegevensbeheerder is verantwoordelijk voor:

- De juistheid, actualiteit en betrouwbaarheid van de gegevens die opgenomen zijn of worden in de gemeentelijke basisadministratie persoonsgegevens.
- Het beheer van documentatie op het gebied van de Wet GBA en overige regelgeving op het gebied van de gemeentelijke basisadministratie persoonsgegevens.
- De communicatie met de afnemers en andere houders van gemeentelijke basisadministraties over gegevensverwerking.

De gegevensbeheerder is bevoegd in overleg met de applicatiebeheerder GBA de gegevensverwerkers aanwijzingen te geven inzake de opname en bijhouding van gegevens in de gemeentelijke basisadministratie persoonsgegevens.

5.4.3 Verantwoordelijkheden van de privacybeheerder GBA

De privacybeheerder is verantwoordelijk voor:

- De inhoudelijke afhandeling van de periodieke gegevensverstrekking die plaatsvindt op basis van een autorisatiebesluit van de Minister van Binnenlandse Zaken Koninkrijksrelaties, alsmede de systematische gegevensverstrekking die plaatsvindt op grond van de door het college van burgemeester en wethouders vastgestelde Verordening gemeentelijke basisadministratie persoonsgegevens.
- Het dagelijkse toezicht op de naleving van de privacyvoorschriften die voortvloeien uit de Wet GBA en de Wet bescherming persoonsgegevens met betrekking tot de hoofdafdeling Dienstverlening.

De privacybeheerder voorziet in:
- De afhandeling van de verzoeken om inzage overeenkomstig artikel 79 van de wet (inzage).
- De behandeling van alle verzoeken om geheimhouding die op basis van artikel 102 lid 1a ingediend worden en doet eventueel de privacytoets van art. 102 lid 2.
- De afhandeling verzoeken om inzage in verstrekkingen aan afnemers en derden.

De privacybeheerder is betrokken bij alle bezwaarschriftenprocedures die voortvloeien uit genomen beslissingen op grond van de wet en daarbij behorende regelingen, de Wet bescherming persoonsgegevens voor zover hierbij privacyaspecten aan de orde zijn.

5.4.4 Verantwoordelijkheden van de applicatiebeheerder GBA

De applicatiebeheerder GBA heeft de volgende taken:

- Verstrekken adviezen aan de leidinggevende over het te voeren beleid met betrekking tot de GBA applicatie(s).
- Zorgdragen voor de beschikbaarheid en kwaliteit van de GBA applicatie(s).
- Optreden als intermediair tussen gebruikers, het managementoverleg en automatiserings- en informatiedeskundigen met betrekking tot de GBA applicatie(s).
- Signaleren van de behoefte aan uitbreiding van apparatuur en overlegt dit met zowel de gegevensbeheerder Dienstverlening als met het afdelingshoofd Informatie en Communicatie Technologie en/of de systeembeheerder.
- Adviseren in geval van daadwerkelijke uitwijk van de GBA applicatie(s).
- Signaleren van het onjuist omgaan met de GBA applicatie(s) en meldt dit aan de leidinggevende zodat deze maatregelen kan nemen om dit te voorkomen.
- Zorgdragen voor de tijdige en kwalitatief goede verwerking van gegevens met behulp van de GBA applicatie(s).
- Zorgdragen voor de tijdige en kwalitatief goede oplevering van informatie uit de GBA applicatie(s).
- In samenwerking met de afdeling Informatie en Communicatie Technologie verzorgen van de acceptatie van nieuwe releases van de GBA applicatie(s).
- Bewaken van een juiste toepassing van de gebruikersprocedures ten aanzien van de GBA applicaties.
- Betrokken bij of verzorgen van de training en begeleiding van de medewerkers op het gebied van de GBA applicatie(s).
- Beheren en onderhouden van de bij de GBA applicatie(s) behorende documentatie.

5.4.5 Verantwoordelijkheden van de systeembeheerder GBA

De systeembeheerder is verantwoordelijk voor het technisch onderhoud van de GBA applicatie(s).

De systeembeheerder voorziet in:
- De fysieke beveiliging van de GBA applicatie(s).

- Een dagelijkse back-up die wordt ondergebracht in een daartoe uitgeruste en beveiligde ruimte op een andere locatie dan de ruimte waarin de GBA-apparatuur is opgesteld.
- De technische installatie van gewijzigde of nieuwe versies van de GBA applicatie(s).
- De beschikbaarheid van de GBA applicatie(s) overeenkomstig hetgeen daarover intern en met derden is overeengekomen.

De systeembeheerder is bevoegd:
- direct maatregelen te treffen als de continuïteit van de GBA applicatie(s) of de daarin opgeslagen informatie acuut in het geding is; hij is verplicht achteraf ter zake te rapporteren aan de informatiebeheerder.
- aanwijzingen te geven over:
  - beheer de GBA applicatie(s).
  - beheer van de bestanden opgenomen in de GBA applicatie(s).
  - reconstructiemaatregelen ten behoeve van de GBA applicatie(s).

5.4.6 Verantwoordelijkheden van de beveiligingsfunctionaris reisdocumenten

In overeenstemming met artikel 93 van de PUN 2001 dient de beveiligingsfunctionaris reisdocumenten door de burgemeester van de gemeente Haarlem te worden aangewezen.

De beveiligingsfunctionaris reisdocumenten moet zijn aangesteld voor het toezicht op de naleving van de beveiligingsprocedures betrekking hebbend op de reisdocumenten. De taken en verantwoordelijkheden dienen te zijn beschreven in een functiebeschrijving.

De beveiligingsfunctionaris reisdocumenten is rechtstreeks verantwoording verschuldigd aan de burgemeester waar het gaat om zijn beveiligingstaken. De beveiligingsfunctionaris reisdocumenten is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van reisdocumenten en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

Van de aanwijzing of de vervanging van de beveiligingsfunctionaris reisdocumenten moet melding worden gedaan aan het agentschap BPR.

5.4.7 Functiebeschrijving van de beveiligingsfunctionaris reisdocumenten

<u>Plaats in de organisatie</u>

Rechtstreekse verantwoordelijkheid naar de burgemeester zonder tussenkomst van leidinggevenden in de lijn. De beveiligingsfunctionaris reisdocumenten is onafhankelijk van de taken en werkprocessen op de hoofdafdeling Dienstverlening.

De beveiligingsfunctionaris reisdocumenten wordt conform de PUN2001 door de burgemeester in deze taak benoemd. Daarbij dient in ieder geval sprake te zijn van functiescheiding tussen de beveiligingsfunctie en uitvoerende taken bij reisdocumenten (in overeenstemming met PUN art. 93 lid 10).

De beveiligingsfunctionaris reisdocumenten is verantwoordelijk voor:
- De controle (steekproefsgewijze tussentijdse controles) op de naleving van de beveiligingsprocessen, -procedures en instructies van reisdocumenten mede aan de hand van Beveiligingsnet.
- Het (laten) verrichten van onderzoek bij incidenten, met het doel dergelijke situaties in de toekomst te voorkomen.
- Het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten/tekortkomingen in de beveiligingsvoorzieningen.

Daarnaast kent deze medewerker de volgende algemene beveiligingstaken met betrekking tot reisdocumenten, waarvoor hij tevens verantwoordelijk is:

- Het bewaken van uit te voeren acties ter verbetering voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van het Informatiebeveiligingsplan GBA en waardedocumenten.
- Er op toezien dat het Informatiebeveiligingsplan GBA en waardedocumenten, beveiligingsprocessen, -procedures/afspraken en instructies actueel worden gehouden.
- Gevraagd en ongevraagd advies geven aan het management over verbeteringen ten aanzien van beveiliging.
- Het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures.
- Het bevorderen van eenduidigheid, efficiency en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar het geven van voorlichting en instructie aan medewerkers door middel van toetsing van de opgestelde beveiligingsprocedures betrekking hebbend op de reisdocumenten in de praktijk.
- Het introduceren en bekendmaken van nieuwe medewerkers met de beveiligingsprocedures betrekking hebbend op de reisdocumenten.

Rapportage en verantwoording

- Het registreren van door de gegevensbeheerder Dienstverlening gedane meldingen van beveiligingsincidenten.
- Rapporteren aan de burgemeester over de stand van zaken van beveiliging en/of naar aanleiding van bijzonderheden.
- Het rapporteren van de uitkomsten van controles en onderzoek.

5.4.8 Verantwoordelijkheden van de Autorisatie Bevoegde Reisdocumenten

De Autorisatie Bevoegde Reisdocumenten (ABR) is de medewerker die bevoegd is om de autorisaties voor reisdocumenten te beheren, dat wil zeggen dat hij/zij:

- Autorisaties uitreikt.
- Autorisaties en eventuele wijzigingen daarin aanmeldt bij de producent.
- Registreert aan wie deze autorisaties zijn verstrekt.
- Toezicht houdt op het zorgvuldig gebruik van deze autorisaties.

5.4.9 Verantwoordelijkheden van de beveiligingsfunctionaris rijbewijzen

Overeenkomstig artikel 128 van het Reglement rijbewijzen dient er een beveiligingsfunctionaris Rijbewijzen door de burgemeester van de gemeente Haarlem te worden aangewezen.

Deze beveiligingsfunctionaris rijbewijzen moet zijn aangesteld voor het beheer en toezicht op de naleving van de beveiligingsprocedures. De taken en verantwoordelijkheden dienen te zijn beschreven in een functiebeschrijving.

De beveiligingsfunctionaris rijbewijzen is rechtstreeks verantwoording verschuldigd aan de burgemeester waar het gaat om zijn beveiligingstaken. De beveiligingsfunctionaris rijbewijzen is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van rijbewijzen en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

5.4.10 Functiebeschrijving van de beveiligingsfunctionaris rijbewijzen

Plaats in de organisatie

Rechtstreekse verantwoordelijkheid naar de burgemeester zonder tussenkomst van leidinggevenden in de lijn. De beveiligingsfunctionaris rijbewijzen is onafhankelijk van de taken en werkprocessen op de hoofdafdeling Dienstverlening.

De beveiligingsfunctionaris rijbewijzen wordt conform het Reglement rijbewijzen (artikel 128) door de burgemeester in deze taak benoemd. Daarbij dient in ieder geval sprake te zijn van functiescheiding tussen de beveiligingsfunctie en uitvoerende taken bij rijbewijzen
(in overeenstemming met RR art. 130).

De beveiligingsfunctionaris rijbewijzen is verantwoordelijk voor:
- De controle (steekproefsgewijze tussentijdse controles) op de naleving van de beveiligingsprocessen, -procedures en instructies van rijbewijzen.
- Het (laten) verrichten van onderzoek bij incidenten, met het doel dergelijke situaties in de toekomst te voorkomen.
- Het naar aanleiding van onderzoek/controles en/of incidenten signaleren van knelpunten/tekortkomingen in de beveiligingsvoorzieningen.

Daarnaast kent deze medewerker de volgende algemene beveiligingstaken met betrekking tot rijbewijzen, waarvoor hij tevens verantwoordelijk is:

- Het bewaken van uit te voeren acties ter verbetering voortkomend uit onderzoek, incidenten of naar aanleiding van de jaarlijkse actualisering van het Informatiebeveiligingsplan GBA en waardedocumenten.
- Er op toezien dat het Informatiebeveiligingsplan GBA en waardedocumenten, beveiligingsprocessen, -procedures/afspraken en instructies actueel worden gehouden.
- Gevraagd en ongevraagd advies geven aan het management over verbeteringen ten aanzien van beveiliging.
- Het adviseren bij het ontwikkelen van nieuwe beveiligingsprocedures en onderhouden/aanpassen van bestaande beveiligingsprocedures.
- Het bevorderen van eenduidigheid, efficiency en effectiviteit ten aanzien van beveiligingsaspecten door het ten minste eenmaal per jaar het geven van voorlichting en instructie aan medewerkers door middel van toetsing van de opgestelde beveiligingsprocedures betrekking hebbend op de reisdocumenten in de praktijk.
- Het introduceren en bekendmaken van nieuwe medewerkers met de beveiligingsprocedures betrekking hebbend op de rijbewijzen.

<u>Rapportage en verantwoording</u>
- Het registreren van door de gegevensbeheerder Dienstverlening gedane meldingen van beveiligingsincidenten.
- Rapporteren aan de burgemeester over de stand van zaken van beveiliging en/of naar aanleiding van bijzonderheden.
- Het rapporteren van de uitkomsten van controles en onderzoek.

5.4.11 Verantwoordelijkheden van de Autorisatie Bevoegde Rijbewijzen

De Autorisatie Bevoegde Rijbewijzen is de medewerker die bevoegd is om de autorisaties voor rijbewijzen te beheren, dat wil zeggen dat hij/zij:

- Autorisaties vernieuwt.
- Autorisaties toevoegt.
- Autorisaties beëindigt.
- Registreert aan wie deze autorisaties zijn verstrekt.
- Toezicht houdt op het zorgvuldig gebruik van deze autorisaties.

5.5 Functiescheiding (Reisdocumenten)

Om de kans te verkleinen dat medewerkers van de hoofdafdeling Dienstverlening door kwaadwillenden worden misleid (externe fraude) of dat zij al dan niet onder druk van chantage, bedreiging of omkoping, misbruik maken van hun bevoegdheden (interne fraude) is functiescheiding bij het verstrekken van waardedocumenten een essentiële voorwaarde.

Alvorens hierop in te gaan een korte uitleg van de relevante termen:

- Aanvraag
  Het betreft hier het bij de balie indienen van een aanvraag voor een waardedocument. Hiertoe dient een aanvraagformulier te worden ingevuld.
- Verstrekking
  Bij verstrekking gaat het om de juridische beslissing tot afgifte van een nieuw reisdocument. De verstrekkende medewerker controleert de aanvraaggegevens die in de reisdocumentenmodule zijn vastgelegd.
- Beheerder van reisdocumenten en waardepapieren
  Hieronder wordt verstaan de medewerker die het beheer draagt over de voorraad gepersonaliseerde reisdocumenten en de rijbewijzen.
- Ontvangstbevoegde
  Hieronder wordt een specifiek aangewezen medewerker verstaan die bevoegd is tot ontvangst van waardepapieren.
- Uitreiking
  Hieronder wordt het feitelijk ter beschikking aan de houder stellen van het op zijn naam gestelde reisdocument of waardepapier verstaan.
- Uitreikbewijs
  Hieronder wordt het formulier verstaan waarop de houder van het nieuwe reisdocument aangeeft het document in ontvangst te hebben genomen. Deze formulieren worden gearchiveerd.

Op grond van de regelgeving met betrekking tot reisdocumenten dient de gemeente Haarlem de volgende functiescheiding te realiseren:

- Tussen de beveiligingsfunctionaris reisdocumenten en uitvoerende en beheertaken met betrekking tot reisdocumenten.
  De beveiligingsfunctionaris reisdocumenten is niet betrokken bij werkprocessen rond reisdocumenten. Dit voorkomt dat de beveiligingsfunctionaris reisdocumenten zijn eigen werk moet controleren.
- Tussen aanvraag en verstrekking van een reisdocument (PUN art. 93 lid 2).
  De aanvraaggegevens worden bij de aanvraag aan de balie gecontroleerd. Ook de medewerker die de aanvraag verzendt naar de producent controleert de gegevens. De signaleringslijst wordt geraadpleegd voordat het nieuwe document verstrekt wordt. De reisdocumentenmodule geeft namelijk automatisch een signalering indien de aanvrager op de signaleringslijst voorkomt, wanneer een aanvraag wordt ingevoerd door de medewerker. Bovendien geeft de reisdocumentenmodule ook een signalering indien de aanvrager niet over een Nederlandse nationaliteit beschikt.
- Tussen verstrekking, uitreiken en beheer van reisdocumenten (PUN art. 93 lid 1c).
  Het reisdocument moet door een andere medewerker worden uitgereikt dan degene die de beslissing op de aanvraag (de verstrekking) heeft genomen. De functiescheiding op dit gebied wordt in de gemeente Haarlem bereikt doordat op het uitreikformulier de paraaf van de medewerker is aangegeven die over de verstrekking heeft beslist. Door de medewerkers wordt er zelf op toegezien dat de uitreiking door een andere medewerker plaatsvindt/de uitreiking plaatsvindt bij de receptie.

Slechts indien dit door een te geringe personele capaciteit onmogelijk is, kan tijdelijk van dit voorschrift worden afgeweken.

Voor die gevallen gelden specifieke voorschriften:

- Vastleggen reden en moment.
- Vastleggen welke medewerkers betrokken waren.
- Bewaren aanvraagformulieren en gegevens over de aldus verstrekte documenten.
- Achteraf controle van het proces.

5.5.1 Verantwoordelijkheden van de beveiligingsfunctionaris reisdocumenten

In overeenstemming met artikel 93 van de PUN 2001 dient de beveiligingsfunctionaris reisdocumenten door de burgemeester van de gemeente Haarlem te worden aangewezen.

De beveiligingsfunctionaris reisdocumenten moet zijn aangesteld voor het beheer en toezicht op de naleving van de beveiligingsprocedures. De taken en verantwoordelijkheden dienen te zijn beschreven in een functiebeschrijving.

De beveiligingsfunctionaris reisdocumenten is rechtstreeks verantwoording verschuldigd aan de burgemeester waar het gaat om zijn beveiligingstaken. De beveiligingsfunctionaris reisdocumenten is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van reisdocumenten en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

Van de aanwijzing of de vervanging van de beveiligingsfunctionaris reisdocumenten moet melding worden gedaan aan het agentschap BPR.

5.5.2 Functiebeschrijving van de beveiligingsfunctionaris reisdocumenten

Plaats in de organisatie

Rechtstreekse verantwoordelijkheid naar de burgemeester zonder tussenkomst van leidinggevenden in de lijn. De beveiligingsfunctionaris reisdocumenten is onafhankelijk van de taken en werkprocessen op de hoofdafdeling Dienstverlening.

Algemene beschrijving
De beveiligingsfunctionaris reisdocumenten wordt conform de PUN2001 door de burgemeester in deze taak benoemd. Daarbij dient in ieder geval sprake te zijn van functiescheiding tussen de beveiligingsfunctie en uitvoerende taken bij reisdocumenten (in overeenstemming met PUN art. 93 lid 10).
De beveiligingsfunctionaris reisdocumenten is verantwoordelijk voor:

- de coördinatie en aansturing van beveiligingsprocessen;
- het beheer van de beveiligingsprocedures c.q. het Informatiebeveiligingsplan;
- (het organiseren van) de controle op de beveiliging van reisdocumenten.

Daarnaast kent deze medewerker de volgende algemene beveiligingstaken waarvoor hij tevens verantwoordelijk is:

- Voorbereiding beveiligingsbeleid en –plan.
- Rapportage (per jaar) over de implementatie aan de directie.
- Rapportage beveiligingsincidenten.
- Het beheer en toezicht op de naleving van de beveiligingsprocedures.
- Het minstens eenmaal per jaar verzorgen van het geven van voorlichting en instructie aan medewerkers door middel van toetsing van de opgestelde beveiligingsprocedures in de praktijk.
- Het introduceren en bekendmaken van nieuwe medewerkers met de beveiligingsprocedures.

De werkzaamheden omvatten tenminste de volgende onderdelen:

Organisatie van de beveiliging

- Het (laten) ontwikkelen van nieuwe beveiligingsprocedures.

- Het (laten) onderhouden/aanpassen van bestaande beveiligingsprocedures.
- Het (laten) bekend maken en toelichten van (nieuwe/gewijzigde) procedures bij medewerkers.
- Het (laten) verzorgen van de beveiligingsonderwerpen tijdens het werkoverleg.
- Het (laten) verzorgen van periodieke voorlichting (tenminste 1x per jaar) op het gebied van beveiliging om het risicobewustzijn op peil te houden/te verhogen.
- Het (laten) maken van een opleidings- c.q. bewustwordingsprogramma voor medewerkers en leidinggevenden op het gebied van beveiliging.
- Overleg binnen de eigen organisatie of met derden indien de te behandelen beveiligingsaspecten raakvlakken vertonen met de beveiliging van reisdocumenten.

Onderzoek naar de status van de beveiliging

- Het steekproefsgewijs (laten) uitvoeren van tussentijdse controles op de beveiliging aan de hand van het BeveiligingsNet.
- Het actualiseren van het beveiligingsplan reisdocumenten op basis van deze controles.
- Het bewaken van de uit te voeren acties voortvloeiende uit dit onderzoek of uit de jaarlijkse actualisering van het Informatiebeveiligingsplan.
- Het (laten) verrichten van onderzoek bij incidenten; doel hiervan is het leren van incidenten, opdat dergelijke situaties in de toekomst kunnen worden voorkomen.

Rapportage en verantwoording

- De uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken.
- Gevaarlijk gedrag medewerker of niet volgen van procedures.
- Onderzoek bij twijfel over de identiteit van een aanvrager.
- Geconstateerde tekortkomingen in de beveiligingsvoorzieningen.
- Wijziging van procedures/afspraken.

5.5.3 Verantwoordelijkheden van de Autorisatie Bevoegde Reisdocumenten

De Autorisatie Bevoegde Reisdocumenten (ABR) is de medewerker die bevoegd is om de autorisaties voor reisdocumenten te beheren, dat wil zeggen dat hij/zij:

- Autorisaties uitreikt.
- De autorisaties en eventuele wijzigingen daarin aanmeldt bij de producent.
- Registreert aan wie welke autorisaties zijn verstrekt.
- Toezicht houdt op het zorgvuldig gebruik van autorisaties.

De medewerker ontvangt een persoonsgebonden identificatiekaart die in combinatie met een pincode toegang tot het reisdocumentenstation geeft. De autorisatiebevoegde pleegt overleg met de beveiligingsfunctionaris reisdocumenten bij het toekennen van autorisaties.

De medewerker van de hoofdafdeling Dienstverlening tekent voor ontvangst van de persoonsgebonden identificatiekaart en bijbehorende pincode. Deze pincode wijzigt de medewerker direct na ontvangst. De autorisatiebevoegde ziet toe op naleving hiervan. De persoonsgebonden identificatiekaarten en pincodes worden nooit uitgeleend of bekend gemaakt aan anderen.

Persoongebonden identificatiekaarten worden altijd gescheiden bewaard van de pincodes en opgeborgen in een beveiligde ruimte.

De autorisatiebevoegde draagt zorg voor vernietiging van de persoonlijke identificatiekaarten, indien deze niet meer worden gebruikt. Deze worden zowel in de lengte als in de breedte doorgeknipt, zodanig dat de chip middendoor wordt gesneden.

Er zijn tenminste twee medewerkers aangewezen als ABR. De ABR legt rechtstreeks verantwoording af aan de burgemeester. Dit is opgenomen in artikel 79 van de PUN 2001.

Van de aanwijzing of vervanging van een ABR wordt direct melding gedaan aan de leverancier en aan het agentschap BPR.

5.6 Functiescheiding (Rijbewijzen)

Op grond van de bepalingen vanuit het Reglement rijbewijzen dient de gemeente Haarlem de volgende functiescheiding te realiseren:

Tussen aanvraag en uitreiken rijbewijzen
Ook bij rijbewijzen dient een functiescheiding te worden gehanteerd tussen het in behandeling nemen van een aanvraag en het uitreiken van een document op de hoofdafdeling Dienstverlening. Zowel de medewerker die de aanvraag in behandeling neemt als de medewerker die het document uitreikt, voeren de betreffende controles uit. Beide medewerkers paraferen het aanvraagformulier voor akkoord.

5.6.1 Verantwoordelijkheden van de beveiligingsfunctionaris Rijbewijzen

Overeenkomstig artikel 128 van het Reglement rijbewijzen dient er een beveiligingsfunctionaris Rijbewijzen door de burgemeester van de gemeente Haarlem te worden aangewezen.

Deze beveiligingsfunctionaris Rijbewijzen moet zijn aangesteld voor het beheer en toezicht op de naleving van de beveiligingsprocedures. De taken en verantwoordelijkheden dienen te zijn beschreven in een functiebeschrijving.

De beveiligingsfunctionaris Rijbewijzen is rechtstreeks verantwoording verschuldigd aan de burgemeester waar het gaat om zijn beveiligingstaken. De beveiligingsfunctionaris Rijbewijzen is onafhankelijk van de taken en werkprocessen met betrekking tot het beheer en de uitgifte van rijbewijzen en heeft voldoende mogelijkheden om zijn taken goed te kunnen vervullen.

5.6.2 Functiebeschrijving van de beveiligingsfunctionaris rijbewijzen

Plaats in de organisatie

Rechtstreekse verantwoordelijkheid naar de burgemeester zonder tussenkomst van leidinggevenden in de lijn. De beveiligingsfunctionaris rijbewijzen is onafhankelijk van de taken en werkprocessen op de hoofdafdeling Dienstverlening.

Algemene beschrijving
De beveiligingsfunctionaris rijbewijzen wordt conform het Reglement rijbewijzen (artikel 128) door de burgemeester in deze taak benoemd. Daarbij dient in ieder geval sprake te zijn van functiescheiding tussen de beveiligingsfunctie en uitvoerende taken bij rijbewijzen
(in overeenstemming met RR art. 130).
De beveiligingsfunctionaris rijbewijzen is verantwoordelijk voor:

- de coördinatie en aansturing van beveiligingsprocessen;
- het beheer van de beveiligingsprocedures c.q. het Informatiebeveiligingsplan;
- (het organiseren van) de controle op de beveiliging van rijbewijzen.

Daarnaast kent deze medewerker de volgende algemene beveiligingstaken waarvoor hij tevens verantwoordelijk is:

- Voorbereiding beveiligingsbeleid en –plan.
- Rapportage (per jaar) over de implementatie aan de directie.
- Rapportage beveiligingsincidenten.
- Het beheer en toezicht op de naleving van de beveiligingsprocedures.
- Het minstens eenmaal per jaar verzorgen van het geven van voorlichting en instructie aan medewerkers door middel van toetsing van de opgestelde beveiligingsprocedures in de praktijk.
- Het introduceren en bekendmaken van nieuwe medewerkers met de beveiligingsprocedures.

De werkzaamheden omvatten tenminste de volgende onderdelen:

Organisatie van de beveiliging

- Het (laten) ontwikkelen van nieuwe beveiligingsprocedures.
- Het (laten) onderhouden/aanpassen van bestaande beveiligingsprocedures.
- Het (laten) bekend maken en toelichten van (nieuwe/gewijzigde) procedures bij medewerkers.
- Het (laten) verzorgen van de beveiligingsonderwerpen tijdens het werkoverleg.
- Het (laten) verzorgen van periodieke voorlichting (tenminste 1x per jaar) op het gebied van beveiliging om het risicobewustzijn op peil te houden/te verhogen.
- Het (laten) maken van een opleidings- c.q. bewustwordingsprogramma voor medewerkers en leidinggevenden op het gebied van beveiliging.
- Overleg binnen de eigen organisatie of met derden indien de te behandelen beveiligingsaspecten raakvlakken vertonen met de beveiliging van rijbewijzen.

Onderzoek naar de status van de beveiliging

- Het steekproefsgewijs (laten) uitvoeren van tussentijdse controles op de beveiliging.
- Het actualiseren van het beveiligingsplan rijbewijzen op basis van deze controles.
- Het bewaken van de uit te voeren acties voortvloeiende uit dit onderzoek of uit de jaarlijkse actualisering van het Informatiebeveiligingsplan.
- Het (laten) verrichten van onderzoek bij incidenten. Doel hiervan is het leren van incidenten, opdat dergelijke situaties in de toekomst kunnen worden voorkomen.

Rapportage en verantwoording

- De uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken.
- Gevaarlijk gedrag medewerker of niet volgen van procedures.
- Onderzoek bij twijfel over de identiteit van een aanvrager.
- Geconstateerde tekortkomingen in de beveiligingsvoorzieningen.
- Wijziging van procedures/afspraken.

5.6.3 Verantwoordelijkheden van de Autorisatie Bevoegde Rijbewijzen

De Autorisatie Bevoegde Rijbewijzen is de medewerker die bevoegd is om de autorisaties voor rijbewijzen te beheren, dat wil zeggen dat hij/zij:

- Autorisaties vernieuwt.
- Autorisaties toevoegt.
- Autorisaties beëindigt .
- Registreert aan wie welke autorisaties zijn verstrekt.
- Toezicht houdt op het zorgvuldig gebruik van autorisaties.

De medewerker ontvangt een persoonsgebonden identificatiekaart die in combinatie met een pincode toegang tot het rijbewijzenstation geeft. De autorisatiebevoegde pleegt overleg met de beveiligingsfunctionaris Rijbewijzen bij het toekennen van autorisaties.

De medewerker van de hoofdafdeling Dienstverlening tekent voor ontvangst van de persoonsgebonden identificatiekaart en bijbehorende pincode. Deze pincode wijzigt de medewerker direct na ontvangst. De autorisatiebevoegde ziet toe op naleving hiervan. De persoonsgebonden identificatiekaarten en pincodes worden nooit uitgeleend of bekend gemaakt aan anderen.

Persoongebonden identificatiekaarten worden altijd gescheiden bewaard van de pincodes en opgeborgen in een beveiligde ruimte.

De autorisatiebevoegde draagt zorg voor terugzending van de persoonlijke identificatiekaarten, indien deze niet meer worden gebruikt. Deze worden vergezeld van de hiertoe beschikbare formulieren teruggestuurd aan de RDW.

Er zijn tenminste twee medewerkers aangewezen als Autorisatie Bevoegde Rijbewijzen. De Autorisatie Bevoegde Rijbewijzen legt rechtstreeks verantwoording af aan de burgemeester.

Van de aanwijzing of vervanging van een Autorisatie Bevoegde Rijbewijzen wordt het daarvoor bedoelde formulier ingevuld en toegezonden aan de RDW.

Procedures beveiligingsplan GBA en waardedocumenten

Procedure Autorisatie tot het systeem
Procedure Back-up van de GBA applicatie
Procedure Correctie
Procedure Gegevensverwerking
Procedure Geheimhouding
Procedure Herstel van mutaties Burgerzaken
Procedure Identificatie en Machtiging
Procedure Inzagerecht
Procedure Ongedaan maken systematische verstrekkingen
Procedure Protocollering
Procedure Restore van de GBA applicatie
Procedure Terugmeldingen
Procedure Verstrekken binnengemeentelijk
Procedure Verstrekken buitengemeentelijk
Procedure Verstrekkingen via alternatief medium
Procedure Back-up en restore RAAS
Procedure Loket Waardedocumenten
Procedure Ontbreken van voldoende functiescheiding
Procedure Ontvangst en beheer waardedocumenten

Bijlagen beveiligingsplan GBA en waardedocumenten
Bijlage Beheerregeling GBA
Bijlage Formulier Autorisaties
Bijlage Formulier Identificatievragen
Bijlage Formulier Onterechte GBA Verstrekkingen
Bijlage Geheimhoudingsverklaring
Bijlage Parafenlijst inzage
Bijlage Privacyreglement GBA
Bijlage Verordening GBA
Bijlage Verstrekkingentabel GBA
Bijlage Aangewezen medewerkers waardedocumenten
Bijlage Activiteitenkalender waardedocumenten
Bijlage Beoordelingsformulier pasfoto FM 2007
Bijlage Extern onderzoek reisdocumenten
Bijlage Formulier terugzenden reisdoc (C10)
Bijlage Fotomatrix
Bijlage Maatregelenanalyse
Bijlage Ontvangstbewijs identificatiekaart
Bijlage Ontvangstlijst waardedocumenten
Bijlage Onvoldoende functiescheiding
Bijlage Uitdraai Beveiligingsnet
Bijlage Verlenging behandelingstermijn
Bijlage Vermissing signaleringsverzoek def 24b
Bijlage Verzoek aanhouding aanvraagreisdoc 8wk
Bijlage Verzoek signalering
Bijlage Wat te doen bij afkeuring fotos
Bijlage Weigering na signalering 24b
Bijlage Weigering paspoort 24b

Rapportages beveiligingsplan GBA en waardedocumenten
Rapportage controle autorisaties
Rapportage controle gegevensverwerking
Rapportage controle inzagerecht
Rapportage controle privacyregelgeving

Rapportage controle rechtmatigheid verstrekkingen
Rapportage test verstrekking alt medium
Rapportage Evaluatie reisdocumenten
Rapportage Evaluatie rijbewijzen
Rapportage Extern onderzoek reisdocumenten 2004
Rapportage Extern onderzoek reisdocumenten 2007

BIJLAGE 1

Lijst van binnengemeentelijke afnemers met een raadpleegmogelijkheid

De volgende dienstonderdelen van de gemeente Haarlem hebben toegang tot de basisadministratie. Genoemde gegevensset is algemeen; specifieke gegevensset volgens autorisatieformulier GBA.

Organisatie onderdeel	Wettelijk kader	Gegevensset
Dienstverlening/Team Balie Dienstverlening/Digiteam Dienstverlening/Flexpool Dienstverlening/PBO (Personen) Dienstverlening/Bedrijfsbureau	Wet GBA, Kieswet, Besluit Burgerlijke Stand, Burgerlijk wetboek, Nationaliteitswetgeving, Wet op de lijkbezorging, Wet justitiële documentatie, Vreemdelingenwet, Paspoortwet en regelgeving rijbewijzen. Wet Inburgering Nieuwkomers	Alle gegevens uit de GBA
Dienstverlening/PBO (Bedrijven en Omgeving)	Huursubsidiewet Huisvestingswet Wet op de huurtoeslag	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Dienstverlening/Team WMO Voorzieningen	Wet Voorzieningen Gehandicapten WMO	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Concernstaf/Bestuur & Management Ondersteuning	Wet Justitiële Documentatie, B&W besluit Toekennen van onderscheidingen en huwelijksjubilarissen. Wet 29/09/1815 Instelling van de Orde van de Nederlandse Leeuw Wet 29/9/1815 instelling van de Orde van Oranje-Nassau en het Besluit van 10 mei 1995, nadere regels Orde van de Nederlandse Leeuw.	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Administratie	Wet Werk en Bijstand	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelenheid/Beleid en Bedrijfsvoering	Wet Werk en Bijstand ROA	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelenheid/Debiteurenbeheer en Fraudebestrijding	Wet werk en Bijstand Wetboek van Strafrecht/Strafverordening	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)

Sociale Zaken en Werkgelegenheid/Werk en Inkomen A en B	Wet werk en Bijstand	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Sociale Zaken en Werkgelegenheid/Schuldhulpverlening en Budgetbeheer	Wet werk en Bijstand	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Doc. Informatievoorziening	Wet GBA art 96	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Juridische Zaken/Rechtsbesch, Schade en Verz& Invordering, Bezwaar en Beroep	WWB, Cras	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Controle en Relatiebeheer/GEO Informatie/Basisregistratie	BAG, BIBOP	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Middelen en Services/Services Financiën/Beheer & Ontwikkeling Fin. Systeem	Wabb	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Politie Kennemerland	HKD, Wet GBA, Politiewet, WPG	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadsbedrijven/Parkeerbeheer	APV	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Jeugd, Onderwijs en Sport/Bureau CARel	Leerplichtwet Leerplichtregeling 1995	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Jeugd, Onderwijs en Sport/Bureau Leerplicht	Leerplichtwet Leerplichtregeling 1995	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Vastgoed/Vastgoedbeheer	Burgerlijk Wetboek	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Stadszaken/Bedrijfsbureau	Woningwet, Awb	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Bedrijfsbureau	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder.	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Bedrijfsbureau/Onderst. Management	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)

Veiligheid, Vergunningen en Handhaving/Bedrijfsbureau/Uitvoering afdeling	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Handhaving Bebouwde Omgeving/Bureau Procesbegeleiding	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Handhaving Bebouwde Omgeving/Bureau Zuid	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Handhaving Openbare Omgeving/Bureau Specifieke Taken	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Veiligheid, Vergunningen en Handhaving/Omgevingsvergunning/ Vergunningverlening	Woningwet, Huisvestingswet, Monumentenwet, APV, Wro (Wet ruimtelijke ontwikkeling), Wet milieubeheer, Wet milieugevaarlijke stoffen, Wet bodembescherming, Wet geluidhinder	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Wijkzaken/Dagelijks Beheer	Wet economische delicten, Awb, Apv	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)
Wijkzaken/Dagelijks Beheer en Techniek	Wet economische delicten, Awb, Apv	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 13, 14 en 15)

ICT	Het waarborgen van een juiste werking van de computer, het netwerk en de applicaties	Toegang tot alle in het systeem aanwezige gegevens.
Woningservice Kennemerland	Huisvestingswet, Woningwet en overeenkomst opgenomen in verordening	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 4, 10, 11, 12, 13, 14 en 15)
GGD Kennemerland	Collegebesluit uitvoering project PHU	Alle in bijlage I.9 van het Logisch Ontwerp GBA genoemde gegevens. (m.u.v. categorie 11, 12, 13, 14 en 15)

De verantwoordelijke (= het College van B&W) kan, indien noodzakelijk nadere aanwijzingen geven met betrekking tot beveiliging en ter bescherming van de persoonlijke levenssfeer.
Alle binnengemeentelijke afnemers beschikken hooguit over een beperkte gedeeltelijke inzage.

Bijlage 2

Systematische verstrekkingen GBA.

Lijst van binnengemeentelijke afdelingen of-diensten die systematische gegevensverstrekkingen krijgen uit de Gemeentelijke Basisadministratie (GBA). Specifieke gegevensset volgens aanvraagformulier verstrekking GBA-gegevens.

Organisatie onderdeel	Wettelijk kader	Gegevensset
Middelen en Services/Documentaire Informatievoorziening	Wet GBA, art. 96	Algemene en verwijsgegevens[1)]
Stadszaken/Jeugd, Onderwijs en Sport/Leerplicht	Wet GBA, art. 96	Algemene en verwijsgegevens[2)]
Soziale Zaken en Welzijn	Wet GBA, art. 96	Algemene en verwijsgegevens[3)]
Stadszaken/Wonen, Welzijn, Gezondheid en Zorg	Wet GBA, art. 96	Algemene gegevens, uitgezonderd persoonsgegevens met indicatie geheimhouding[4)]
Regiopolitie Kennemerland	Wet GBA, art. 96	Algemene gegevens van overledenen[5)]

BIJLAGE 3

Lijst van binnengemeentelijke afnemers waaraan, met het oog op het met elkaar in verband brengen van verwerkingen van persoonsgegevens, gegevens uit de GBA worden verstrekt.

Wie (afnemers)	Waarvoor	Gegevensset
Sociale Zaken en Welzijn	Basisregistratiesysteem DDS/applicatie GWS4all	Alle mutatiegegevens
Stadszaken/Jeugd, Onderwijs en Sport/Leerplicht	CARel (Centrale administratie RMC en Leerplicht)	Alle mutatiegegevens
Middelen en Services/Documentaire Informatievoorziening	VERSEON	Alle mutatiegegevens

BIJLAGE 4

Lijst van vrije derden waaraan gegevens worden verstrekt.

Wie	Waarvoor	Welke categorie	Welke gegevens	Geheimhouding	Leges	Basis
Bibliotheek (geen onderdeel van de gemeente)	Voor de bijhouding van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Buitenlandse EU-overheden	Ter uitvoering van de opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Buitenlandse niet EU-overheden (met passend beschermingsniveau met betrekking tot persoonsgegevens) www.cbpweb.nl	Ter uitvoering van de opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA Art. 76 WBP
Buitenlandse vertegenwoordigingen hier te lande	Ter uitvoering van de opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Bureau voor Rechtshulp	Ter uitvoering van de opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Crematoria, begraafplaatsen (niet-gemeentelijke)	Voor de bijhouding van registraties verband houdende met het begraven en cremeren.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Culturele organisaties	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Fondsverwervende organisaties	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Inburgeringsbureaus	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Instellingen/organisaties ten behoeve van: -Maatschappelijke dienstverlening -Algemene/geestelijke gezondheidszorg -Kinderopvang -Jeugdwelzijnswerk -Ouderenzorg -Gehandicaptenzorg -Werkvoorziening	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Juridisch loket (Indien de vraag komt van een advocaat van het Juridisch loket t.b.v. een gerechtelijke procedure = verplichte berde)	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Kerken (niet zijnde de SILA)	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Kredietbank (privaatrechtelijk, bijvoorbeeld een stichting)	Voor de aan deze organisatie opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Migrantenorganisaties	Voor het bijhouden van	Vrije	Maximaal de gegevens	Mogelijk	Ja	Art. 100 Wet

Wie	Waarvoor	Welke categorie	Welke gegevens	Geheimhouding	Leges	Basis
	de ledenadministratie	derde	genoemd in art. 100, lid 2 Wet GBA			GBA
Natuurlijke personen	Vooraf schriftelijke toestemming betrokkene (persoon/gezaghouder)	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Ouderenorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Patiëntenverenigingen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Pensioenfondsen (tenzij art. 34 Pensioen- en Spaarfondsenwet van toepassing is)	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja[1]	Art. 100 Wet GBA
Plaatselijke afdelingen van politieke partijen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Reclassering/verslaafden-zorg	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Sportorganisaties en -verenigingen	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Thuiszorgorganisaties	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Vakorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Verenigingen en stichtingen met maatschappelijk of filantropisch doel	Voor de aan deze organisaties opgedragen taken.	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Vrouwenorganisaties	Voor het bijhouden van de ledenadministratie	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Woningbouwverenigingen/woningcorporaties in Haarlem	Ten behoeve van de bijhouding van de huurdersadministratie en de woningtoewijzing	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA
Ziekenhuizen	Voor het uitoefenen van patiëntenzorg, het verlenen van medische zorg en het innen van rekeningen ivm die zorg	Vrije derde	Maximaal de gegevens genoemd in art. 100, lid 2 Wet GBA	Mogelijk	Ja	Art. 100 Wet GBA

Bijlage Privacyreglement GBA

Toelichting op het GBA privacyreglement van de gemeente Haarlem

Met ingang van 1 april 2007 is de wet gemeentelijke basisadministratie persoonsgegevens (GBA) op een aantal punten gewijzigd. Afnemers worden verplicht de in het Besluit GBA aangewezen authentieke persoonsgegevens te gebruiken bij hun beslissingen en bij gerede twijfel omtrent de juistheid van deze gegevens dit aan gemeenten terug te melden.
Voor de binnengemeentelijke verstrekking van GBA-gegevens dient een verordening aanwezig te zijn. Deze verordening bevat ook een voorziening voor de verstrekking aan zogenaamde vrije derden, bedoeld in artikel 100 van de wet GBA.
Er is op …. een nieuwe verordening vastgesteld waarin de gemeenteraad het college van burgemeester en wethouders aanwijst om in een apart reglement deze zaken te regelen. De bepalingen in deze Verordening worden in onderstaand Reglement uitgewerkt.

PRIVACYREGLEMENT GBA

Burgemeester en wethouders van de gemeente Haarlem

gelet op de Wet gemeentelijke basisadministratie persoonsgegevens en op de Verordening gemeentelijke basisadministratie persoonsgegevens

besluiten:

Het Reglement voor de gemeentelijke basisadministratie persoonsgegevens van de gemeente Haarlem vast te stellen

Artikel 1 Begripsbepalingen

Dit reglement verstaat onder:

a. wet: de Wet gemeentelijke basisadministratie persoonsgegevens;

b. verordening: de Verordening gemeentelijke basisadministratie persoonsgegevens, vastgesteld door de gemeenteraad d.d ;

c. verantwoordelijke: het college van burgemeester en wethouders;

d. beheerder: een daartoe ingevolge de beheerregeling, bedoeld in artikel 14 van de wet, aangewezen gemeenteambtenaar of diens plaatsvervanger die is belast met het beheer van de gemeentelijke basisadministratie persoonsgegevens;

e. bewerker: degene die, niet werkzaam binnen de gemeentelijke organisatie, het geheel of een gedeelte van het geautomatiseerde systeem onder zich heeft waarmee de gemeentelijke basisadministratie persoonsgegevens wordt gevoerd;

f. ingeschrevene: degene ten aanzien van wie een persoonslijst als bedoeld in artikel 1 van de wet, in de gemeentelijke basisadministratie persoonsgegevens van de gemeente is opgenomen;

g. binnengemeentelijke afnemer: binnengemeentelijke afnemer als bedoeld in artikel 1 van de wet.

Artikel 2 Beheer van de gemeentelijke basisadministratie persoonsgegevens

1. Beheerder van de gemeentelijke basisadministratie persoonsgegevens is de functionaris als bedoeld in artikel 1 onder d.
2. De beheerder is bevoegd nadere invulling te geven aan:
   a. (te leggen) verbanden met andere gemeentelijke registraties;
   b. (rechtstreekse) toegang tot de basisadministratie middels andere geautomatiseerde toepassingen;
   c. verstrekkingen aan binnengemeentelijke afnemers of daaraan gelijkgestelden, die geen rechtstreekse toegang hebben tot de basisadministratie;

Artikel 3 Authentieke gegevens

Met inachtneming van het bepaalde in de artikelen 4, 5 en 6, worden gegevens verstrekt aan alle binnengemeentelijke afnemers die gegevens uit de GBA nodig hebben voor de vervulling van hun taken, zodanig dat deze afnemers aan hun verplichtingen krachtens de artikelen 3b en 62 van de wet kunnen voldoen.

Artikel 4 Rechtstreekse toegang tot de bevolkingsadministratie

1. Rechtstreekse toegang tot de bevolkingsadministratie hebben:
   a. de beheerder en de door hem aangewezen medewerkers van de hoofdafdeling Dienstverlening;
   b. voor zover niet in een convenant geregeld en voor zover met inachtneming van de artikelen 88 en 89 van de wet de in Bijlage 1 bij dit reglement vermelde binnengemeentelijke afnemers.
2. De in bijlage 1 genoemde binnengemeentelijke afnemers hebben rechtstreekse toegang tot de in die bijlage vermelde gegevens. Zij mogen deze gegevens slechts gebruiken voor de uitvoering van de hun bij wet of door het gemeentebestuur opgedragen taken.

3. Zij hebben de richtlijnen van de beheerder met betrekking tot beveiliging en bescherming van de persoonlijke levenssfeer op te volgen.

Artikel 5 Verstrekking aan binnengemeentelijke afnemers

Met inachtneming van de artikelen 88 en 89 van de wet worden aan de in Bijlage 2 vermelde binnengemeentelijke afnemers die geen rechtstreekse toegang hebben tot de gemeentelijke basisadministratie persoonsgegevens de in die tabel aangegeven gegevens systematisch verstrekt ten behoeve van de eveneens in die tabel aangegeven doeleinden.

Artikel 6 Verbanden met andere gemeentelijke registraties

1. Op grond van artikel 96 van de wet, met het oog op het met elkaar in verband brengen, van verwerkingen van persoonsgegevens, worden aan de in Bijlage 3 beheerders van andere gemeentelijke registraties gegevens verstrekt.
2. De betreffende gegevens kunnen in een convenant worden vastgelegd.

Artikel 7 Telefonische verzoeken om gegevensverstrekking

Aan buitengemeentelijke afnemers, verplichte derden, als bedoeld in artikel 98 van de wet, en andere gemeenten worden telefonisch slechts in bijzondere omstandigheden, ter beoordeling van de beheerder, inlichtingen verstrekt.

Artikel 8 Overige verstrekkingen en de gegevens die kunnen worden verstrekt

Met inachtneming van artikel 100, tweede lid van de wet kunnen, in andere gevallen dan bedoeld in de artikelen 98 en 99 van de wet, aan de in Bijlage 4 bij deze verordening aan te geven overige verzoekers gegevens worden verstrekt voor wat betreft de daarbij aangegeven gegevens en uitsluitend voor de daarbij aangegeven doeleinden en voor zover de persoonlijke levenssfeer daardoor niet onevenredig wordt geschaad.

Artikel 9 Terugmeldplicht

1. Een binnengemeentelijke afnemer die gerede twijfel heeft over de juistheid van een authentiek gegeven dat hij verstrekt heeft gekregen uit de basisadministratie, doet hiervan mededeling aan de beheerder.
2. In Bijlage 5 worden de binnengemeentelijke afnemers aangewezen die tevens mededeling doen in verband met andere dan authentieke gegevens die aan hen verstrekt zijn. Aangegeven wordt welke gegevens het betreft.

Artikel 10 Beveiliging

De beheerder treft ten behoeve van de technische en organisatorische beveiliging de maatregelen als vermeld in het vastgestelde beveiligingsplan.

Artikel 11 Slotbepaling

1. Dit reglement wordt aangehaald als “privacyreglement GBA”.
2. Het reglement ligt ter inzage in het gemeentehuis.

Burgemeester en wethouders van de gemeente Haarlem,

de secretaris,	de burgemeester,
De heer drs. W.J. Sleddering	De heer mr. B.B. Schneiders