Oplegvel Collegebesluit

Portefeuille J. Nieuwenburg
Auteur Mevr. A.L. van der Kraan
Telefoon 5114061 E-mail: alkraan@haarlem.nl
SZW/BB Reg.nr. SZW/BB/2010/365550
Te kopiëren:
B & W-vergadering van 30 november 2010

Onderwerp
Beveiligingsplan SZW

DOEL: Besluiten

Op grond van de Regeling *Structuur uitvoeringsorganisatie werk en inkomen (*Suwi), artikel 6.4: Beveiliging elektronische voorzieningen SUWI is het college bevoegd en verplicht om een beveiligingplan op te stellen.

artikel 6.4: regeling SUWI:
Lid 1: Het UWV, de SVB, de colleges van burgemeester en wethouders, het IB en op de gezamenlijke elektronische voorzieningen SUWI aangesloten niet SUWI-partijen dragen zorg voor de beveiliging van de gegevensuitwisselingen die plaatsvinden in het kader van de gezamenlijke elektronische voorzieningen SUWI, tegen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid, overeenkomstig hetgeen over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I ('Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI').
Lid 2: Het UWV, de SVB, de colleges van burgmeester en wethouders, het IB en op de gezamenlijke elektronische voorzieningen SUWI aangesloten niet- SUWI- partijen geven ieder in een beveiligingsplan aan op welke wijze zij invulling geven aan het eerste lid.

B&W

1. Het college stelt de Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid vast.
2. Het college stemt in met de Functieverdeling zoals opgesteld in bijlage 4.
3. Het besluit heeft geen financiële consequenties.

Collegebesluit

Onderwerp: Beveiligingsplan SZW
Reg. Nummer: SZW/BB/2010/365550

1. Inleiding
Een organisatie als de gemeente Haarlem is constant bezig met het vastleggen en beheren van informatie. De gemeente is veelal verantwoordelijk voor de kwaliteit van deze informatie. Kwalitatief goede informatie is informatie die volledig, juist en tijdig beschikbaar wordt gesteld aan medewerkers en (in beperkte mate aan) burgers. Deze informatie kan alleen worden ingezien en aangepast door medewerkers en burgers die daartoe bevoegd zijn en is altijd op te vragen wanneer het noodzakelijk is. Informatiebeveiliging is juist hierop gericht. Niet alleen heeft de gemeente Haarlem zelf een verantwoordelijkheid om de beveiliging van informatie en informatiesystemen adequaat te regelen, ook de wetgever stelt steeds meer eisen als het gaat om informatiebeveiliging. Zo is deze voor Sociale Zaken en Werkgelegenheid vastgelegd in de SUWI regeling en de Wet Bescherming Persoonsgegevens.

Het beheersen van de risico's die samenhangen met informatie en informatiesystemen (informatiebeveiliging) is een belangrijk aandachtsgebied. De schade als gevolg van incidenten/calamiteiten kan aanzienlijk zijn.

Afdeling Sociale Zaken en Werkgelegenheid heeft een beveiligingplan geformuleerd om de risico's in kaart te brengen en vervolgstappen te definiëren om een duurzame doch flexibele basis voor de toekomst neer te leggen.

2. Besluitpunten college
1. Het college stelt de Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid vast.
2. Het college stemt met de Functieverdeling zoals opgesteld in bijlage 4.

3. Beoogd resultaat
Voldoen aan wettelijk gestelde eis van het hebben van een actueel beveiligingsplan op grond van de Wet Suwi.
Werkwijze in overeenstemming brengen met het beveiligingsplan

4. Argumenten
Het voorstel voorziet in de wettelijke eisen.

5. Kanttekeningen
Uit de managementsamenvatting komen de volgende aandachtspunten naar voren:
a) Binnen de afdeling Sociale Zaken en Werkgelegenheid van de gemeente Haarlem is er onvoldoende beveiligingsbewustzijn.
b) Er is geen uitwijkvoorziening voor de applicaties van Sociale Zaken en Werkgelegenheid.
c) Er is geen aggregaat op de locatie Zijlsingel aanwezig.
d) Het netwerk van de gemeente Haarlem is te transparant waardoor de mogelijkheid om het netwerk te infecteren met een virus een reële bedreiging vormt.

6. Uitvoering
Bij het beheer van bevoegdheden gebruik te maken van Suwinet, overige informatiesystemen van SZW en het gemeentebrede netwerk wordt te weinig aandacht besteed aan het tijdig verwijderen van niet meer actieve accounts. Hiervoor zal een striktere procedure worden ontwikkeld.

SZW gaat punt a van de kanttekeningen oppakken.

De punten b, c en d uit de kanttekeningen zullen door ICT worden opgenomen, deze zaken worden meegenomen in de algehele opzet van de infrastructuur tbv de nieuwe huisvesting waarvoor een budget is gereserveerd.

7. Bijlagen
A. Ricico-inventarisatie en evaluatie; Informatiebeveiliging Sociale Zaken en Werkgelegenheid (ter inzage)
B. Managementsamenvatting; Beveiliging binnen Sociale Zaken en Werkgelegenheid (ter inzage)
C. Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid (ter inzage)
D. Bijlage 2; Beheerregeling applicaties van Sociale Zaken en Werkgelegenheid Gemeente Haarlem (ter inzage)
E. Bijlage 4; Functieverdeling (ter inzage)

Het college van burgemeester en wethouders

de secretaris de burgemeester

Risico-inventarisatie en evaluatie Informatiebeveiliging Sociale Zaken en Werkgelegenheid

---

Gemeente Haarlem

Versie :1.0 Definitief
Auteur :de heer M. van Schoonhoven
Proces verantwoordelijke :de heer R.J.A. van Noort
Datum :30 juni 2010
Bestuur en Management Consultants (BMC)

Inhoudsopgave

1 Risico analyse

1.1 Inleiding

Het optreden van een gebeurtenis welke, bij het ontbreken van passende maatregelen, duidelijk waarneembare gevolgen (materieel dan wel immaterieel) voor de organisatie heeft, noemen we een calamiteit. Calamiteiten zijn niet uit te sluiten daar het niet mogelijk is om voor alle mogelijk gebeurtenissen beheersmaatregelen te treffen. Daarnaast dient in ogenschouw te worden genomen dat beheersmaatregelen tijd en geld kosten zowel bij de opzet als in het onderhoud. Het is dus van belang om een goede analyse te maken van de calamiteiten die in de organisatie kunnen optreden om zodoende de juiste maatregelen te kunnen treffen.

Risico's zijn altijd gerelateerd aan de doelstelling van de organisatie. Daar veel diensten en producten afhankelijk zijn van de informatievoorziening is het van belang om een goede analyse te maken.
De risico's die een organisatie loopt t.a.v. de informatiebeveiliging zijn in veel gevallen gelijk. De onderstaande risico's kunnen worden onderkend:

- De klant[1] krijgt geen informatie
- De klant krijgt niet tijdig de gewenste informatie
- De klant krijgt verkeerde informatie
- De klant krijgt onvolledige informatie
- Vertrouwelijke informatie komt in verkeerde handen

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

- Vitale informatie gaat verloren.
- Controle is niet meer mogelijk.
- Informatie is niet meer beschikbaar.
- Goederen en diensten kunnen niet geleverd worden.
- Demotivatie bij medewerkers.
- Chaos.
- Fraude.
- Vertrouwelijke informatie lekt uit.

[1] Met klant bedoelen we zowel de interne als de externe klant.

1.2 Het hoe en waarom van een risico analyse

Voordat de uitgangspunten waaraan de informatiebeveiliging moet voldoen bepaald worden, wordt een risico analyse inclusief een gevolgschade onderzoek uitgevoerd om de risico's voor de bedrijfsprocessen te analyseren. Later kunnen dan voor de kritieke bedrijfsprocessen de kans van optreden (waarschijnlijkheid) of de mogelijke schade (het effect) worden weggenomen of beperkt. Wordt deze analyse overgeslagen dan worden maatregelen gekozen welke wellicht het beoogde doel niet waarborgen.

Een *risico analyse* 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 risico analyse 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 het directieteam 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 het directieteam vervolgens keuzen maken welke risico's men wil kunnen overleven.
Deze methode levert meer 'tastbare' handvatten. het directieteam ziet hierdoor in een oogopslag welke processen de hoogste prioriteit dienen te krijgen. De kwalitatieve methode wordt in het voorliggend Informatiebeveiligingsplan toegepast.

1.3 Waarschijnlijkheid en effect

Om de beveiliging verder te verbeteren, moet een risico analyse worden uitgevoerd. Er dient eerst bewustwording te zijn voordat men adequate maatregelen kan treffen.

Er zijn een aantal generieke bedreigingen die kunnen worden onderscheiden tav de informatiebeveiliging. Er wordt een drietal bedreigingen onderscheiden:

- Personele bedreigingen
- Fysieke bedreigingen
- Technische bedreigingen

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 risico analyse 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 bij het publiek.

1.4 Prioriteitstelling

De risico's zijn in de risicoanalyse ten opzichte van elkaar gewogen op de aspecten "waarschijnlijkheid" en "effect" conform de CRAMM methode. 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 werkelijke risico (R) van een incident is het product van waarschijnlijkheid (W) en effect (E):
R = W x E.
Op basis van het risico wordt de prioriteit bepaald van de noodzaak dit risico te verminderen.

Het informatiebeveiligingsbeleid van de gemeente Haarlem stelt dat de beschikbaarheid van de gegevensprocessen moet zijn afgestemd op het betreffende bedrijfsproces. In dit kader zijn technische en organisatorische maatregelen noodzakelijk om een passend beveiligingsniveau te bereiken.
Deze maatregelen moeten zijn gebaseerd op een zorgvuldige risico analyse, waarbij de lokale 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 risico analyse uitgevoerd met de leden van de beveiligingscoördinator van de gemeente Haarlem.

Met de beveiligingswerkgroep SUWI is op 30 juni 2010 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.

1.5 Analyse matrix

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
Onjuistheden	• Fouten in handmatige invoer • Fouten in externe aanlevering • Systeemfout	• Procedure Gegevensverwerking • Rapportage controle gegevensverwerking • Procedure Correctie • Procedure Terugmeldingen. • Matrices GWS4all	1	1	1					
Onvolledigheden	• Fouten in handmatige invoer • Fouten in externe aanlevering • Systeemfout	• Procedure Gegevensverwerking • Rapportage controle gegevensverwerking • Matrices GWS4all	1	1	1					
Niet beschikbaar	• Technische Uitval • Menselijke fout • Personeelstekort • Fysieke belemmeringen • Procedure continuïteitsbeheer	• Bijlage Onderhoudscontract • Bijlage Kenmerken SUWI systeem • Procedure Back-up van de SUWI applicatie • Procedure 6 Continuïteitsbeheer • Procedure Restore van de SUWI applicatie • Procedure Herstel van mutaties GWS • Bijlage Formulier Registratie Reconstructie • Rapportage test restore • Rapportage test reconstructie • Bijlage Uitwijkcontract • Rapportage test	2	3	6	2	In het geval van een calamiteit is er bij een uitwijk geen GWS4all beschikbaar Geen aggregaat voor serverruimte	Uitwijk GWS4ALL inrichten. Meenemen in nieuwe vestiging	? Medio 2011	

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
		uitwijk								
Niet Controleerbaar	• Vastlegging van procedures • Vastlegging van taken, bevoegdheden en verantwoordelijkheden (functiescheiding) • Logging	• Verantwoordelijkheden gemeentebestuur • Rapportage evaluatie beveiligingsbeleid en plan • Bijlage Functieverdeling • Bijlage Uitdraai Beveiligingsnet • Procedure Communicatie over beveiliging • Procedure Protocollering • Rapportage controle rechtmatigheid verstrekkingen • Procedure 10 Instellen en opvragen auditlog	2	2	4					
Vertrouwelijkheid / Uitlekken	• Interne uitwisseling • Externe uitwisseling (partner / vrienden) • Elektronisch (verkeerd mailadres) • Papier (verkeerd adres) / Prullenbakken / Papiercontainer / Laten slingeren • Hoe is de fysieke bescherming geregeld	• Bijlage Kenmerken Gemeentelijke LAN • Bijlage Kenmerken fysieke beveiliging • Bijlage Formulier Autorisaties • Bijlage Geheimhoudingsverklaring • Procedure Verstrekkingen via alternatief medium • Ambtseed • Rapportage controle privacyregelgeving	2	2	4			Aandacht voor beveiligingsbewustzijn.	Okt 2010	MT Sociale Zaken en Werkgelegenheid

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
	• Wat mogen technische applicatiebeheerders en systeembeheerders • Hoe gaan mensen in de organisatie om met vertrouwelijke gegeven (roddelcultuur)	• Rapportage controle rechtmatigheid verstrekkingen • Rapportage controle autorisaties • Rapportage test verstrekking alt medium • Procedure Autorisatie tot het systeem • Clean desk policy wordt onder de aandacht gebracht middels 'project Digitalisering Cliëntdossier'								
Brand	• Bouwmateriaal gebouw • Materiaal dakbedekking • Leeftijd gebouw • Vrijstaand of buren • Wat zit in de • omgeving	• Brandmelders • Brandhaspels • Brandblussers • Branddetectie • Inspectie Brandweer	1	3	3					
Explosie	• Gasaansluiting • Wat zit in de omgeving		1	3	3					
Bliksem	• Bliksemafleider • Overspanningbeveiliging	• Bliksemafleiders	1	3	3					

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
Stof, vuil en water	• Hoe zijn kritische onderdelen gepositioneerd in het gebouw. • Maatregelen computerruimte (stofafzuiging)		1	2	2					
Klimaat beheersing	• Hoe is de koeling geregeld van de werkruimte (concentratiestoringen) o Hoe is de koeling geregeld van de computerruimte (zit deze op het	• Bijlage Kenmerken Computerruimte	1	4	4					
Stroomstoring	• Is er een noodstroom voorziening • Wat is hierop aangesloten	• UPS	2	4	8	1	Geen aggregaat voor publieksdienst	Meenemen in nieuwe vestiging	Medio 2011	?
Hardware storingen	• Hoe is het wijzigingenbeheer geregeld • Hoe is het incidenten beheer geregeld • Hoe is het probleembeheer geregeld • Welke continuïteitsmaatregelen zijn getroffen • Hoe is de uitwijk geregeld	• Bijlage Kenmerken Computerruimte	1	4	4					

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
Software storingen	• Hoe is het testproces geregeld. • In hoeverre zijn storingen te achterhalen (logging). • Welke continuïteitsmaatregelen zijn getroffen • Welke maatregelen tav bestandsherstel zijn er getroffen • Welke maatregelen		2	4	8	1				
Lekkage	• Wat is de leeftijd van het gebouw (oude leidingen) • Hoe zijn kritische onderdelen gepositioneerd • Airco leidingen		1	2	2					
Inbraak	• Welke maatregelen in preventieve sfeer (braak werend glas / camera's / detectie) • Wat staat er voor het raam?	Camera's Toegangsbeveiliging Braakwerend glas PC waar mogelijk uit het zicht geplaatst Melkglas aan straatzijde	1	1	1					
Diefstal	• Welke maatregelen in preventieve sfeer camera's / kluis / kasten / controle waardevolle goederen) • Staan er waardevolle	Kamers zijn af te sluiten middels normaal hang en sluitwerk Camera's Alarm installatie	2	2	4		Eenmaal door een deur (sluis) is het pand vrij toegankelijk en kan het ook zonder pas/sleutel worden	Aandachtspunt bij nieuwe huisvesting	Medio 2011	?

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
Overval	• Welke maatregelen in preventieve sfeer camera's / noodknop) • Waarde beperking	Camera's in publieke gedeelte Fysieke toegangsbeveiliging Interventieteams	1	4	4					
Sabotage	• Medewerker tevredenheid (reorganisatie?) • Motivatie • Sociale controle • Systeem van interne controle		1	4	4					
Virussen	• Aansluitmogelijkheden op het systeem (USB / Externe harddisk) • Draadloos netwerk • Virus controle (heuristisch of via signature)	• Virusscanner	1	3	3					
Hacking	• Heeft er een test plaatsgevonden op de firewall en de website? • Wordt de firewall extern gehost? • Wordt de firewall door externen onderhouden?	• Hack-test / poortcontrole • Gemnet	1	4	4					

Bedreiging	Suggesties	Getroffen maatregel	Waarschijnlijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
Externe fraude	• Hoe zijn de controle maatregelen rond het verkrijgen van een uitkering, • Signalering uitkeringsfraude (sociale recherche).	• Functie scheiding • Procedure verstrekking uitkering • Controle maatregelen / Handhaving	2	4	8	1				
Interne fraude	• Hoe zijn de controle maatregelen rond de kritische processen geregeld • Preventie samenspanning	• Procedure inlog SUWI • Procedure inlog GWS4all • Formulier nieuwe medewerker • Procedure indiensttreding nieuwe medewerker	2	3	6	2		Opstellen Procedure uitdiensttreding medewerker. Met name het afmelden van de autorisaties speelt hierbij een belangrijke rol		MT SZW
Ongeautoriseerd gebruik systeem	• Is er een adequate toegangsprocedure • Voorziet P&O in informatie omtrent instroom, doorstroom en uitstroom van medewerkers.	• Op eigen initiatief wordt er wat gedaan met doorstroom. • Procedure inlog GWS4all • Procedure inlog SUWI	2	3	6	2		Opstellen Procedure uitdiensttreding medewerker. Met name het afmelden van de autorisaties speelt hierbij een belangrijke rol		MT SZW
Fysiek geweld	• Hoe zijn mensen beschermd tegen bezoekers (noodknop)	• Noodknop • Beveiliger • Agressieprotocol • Training • Werkplekken niet toegankelijk	1	4	4					

Bedreiging	Suggesties	Getroffen maatregel	Waarschijn lijkheid	Effect	Risico	Prio-riteit	Rest risico	Nog te nemen maatregelen	planning	Verant-woordelijke
Verbaal geweld	• Hoe zijn mensen hierin getraind	• Noodknop • Beveiliger • Agressieprotocol • Training • Werkplekken niet toegankelijk Periodieke bijscholing	1	4	4					
Kwantitatieve onderbezetting	• Hoeveel personen zijn per functie beschikbaar (hou rekening met ziekt e en verlof)	• Voldoende personeel soza.	1	2	2					
Kwalitatieve onderbezetting	• Ervaringsniveau • Opleidingsniveau	• Opleiding en bijscholing soza is geregeld. • Kwaliteitsmedewerke rs koppelen verbetermogelijkhede	1	2	2					
Vandalisme	• Welke preventieve maatregelen zijn getroffen	• Beveiligpersoneel overdag	1	4	4					
Onbevoegde aanwezigheid	• Hoe is de fysieke toegangsbeveiliging geregeld • Is er een bezoekersregeling • Is er een afsluitcontrole	• Druppels (proximity token) zowel voor naar binnen als naar buiten gaan. Kritische ruimtes zijn extra beveiligd alleen toegang geautoriseerd personeel	1	1	1					

1.6 Toelichting op de analyse

Voor een groot aantal bevindingen geldt dat de waarschijnlijkheid en soms mede daardoor het risico in deze voor de gemeente Haarlem onbeduidend tot gering zijn.

Een onmisbaar element in de keten van maatregelen die de vereiste kwaliteit moet waarborgen, is dat achteraf getoetst kan worden of de handeling door of met behulp van SUWI juist is verricht. Protocollering binnen Sociale Zaken en Werkgelegenheid is niets meer en niets minder dan de laatste schakel in de kwaliteitsketen.
Heeft het systeem correct gefunctioneerd en heeft de verstrekking rechtmatig plaatsgevonden. Tijdens de gesprekken is aangegeven dat deze controles worden uitgevoerd, echter zonder vastlegging van de uitgevoerde handeling. Zonder protocollering zijn deze vragen in het algemeen niet te beantwoorden. Het is daarom van groot belang dat de processen en procedures binnen de gemeente Haarlem worden vastgelegd en gecontroleerd. Naast het beschrijven van de processen en procedures is het van belang dat medewerkers van de gemeente Haarlem op de hoogte worden gesteld van deze processen en procedures. Hiermee verhogen we het bewustzijn in kennis, houding en gedrag van de medewerkers over informatiebeveiliging en minimaliseren we de beveiligingsrisico's. Het verdient aanbeveling periodiek het onderwerp beveiliging aan de orde te stellen tijdens een werkoverleg en/of speciale informatie sessies.

Van de meeste bedreigingen kan op grond van de kennis en ervaring van de geïnterviewden worden gesteld dat deze qua kans van optreden en mogelijke schade gering zijn.

Uit de analyse komen punten naar voren waarvan de score dermate hoog is dat hiervoor aanvullende maatregelen nodig geacht worden. Deze punten zijn:

1. <u>Externe Fraude</u>
   Ten alle tijden moet voorkomen worden dat er een negatieve houding in de samenleving ontstaat voor het verstrekken van uitkeringen. Het is daarom aan de gemeente goed Handhavingsbeleid op te stellen. Handhavingsbeleid schept preventieve en curatieve randvoorwaarden teneinde misbruik en oneigenlijk gebruik tegen te gaan bij het uitvoeren van de bijstandswet. Het bestrijden en voorkomen van misbruik, ofwel handhaving is een belangrijke voorwaarde in het kader van de inkomenswaarborg. Een adequaat ingerichte uitvoeringsorganisatie waarbinnen men alert is op fraude, draagt bij aan het terugdringen van misbruik.

   Onder handhaving valt al het beleid dat gericht is op beperking van misbruik en oneigenlijk gebruik van de regelingen. Hierbij kan onderscheid gemaakt worden tussen preventief beleid, repressief beleid en interne controle.

   Uit de gespreken die zijn gevoerd is het beeld ontstaan dat de gemeente Haarlem Zowel prefentief als repressief de nodige maatregelen heeft getroffen, dit heeft zicht ook vertaald in een lage score op de waarschijnlijkheid. Echter als zich een fraude geval voor doet en dit publiekelijk bekend wordt heeft dit een groot effect op het imago van de gemeent Haarlem. Aandacht op dit onderdeel is daarom blijvend geboden. Maatregelen die worden voorsteld hebben een preventief karakter.
   <u>Voorgestelde maatregelen:</u>
   - Preventie doormiddel van voorlichting, mondeling maar ook via brochures, Maak in een brochure aan klanten duidelijk hoe de gemeente Haarlem met fraudeurs om gaat.
   - Werken met risicoprofielen, er zijn klanten die zich in omstandigheden bevinden waarbij het risico op fraude groter is.

2. Softwarestoringen
   Virussen en malware kunnen schade toebrengen aan de systemen en de databases van de gemeente Haarlem. Een van de oorzaak hiervan zit in het feit dat USB aansluitingen in vele gevallen open staan en aangesloten apparatuur niet afdoende gescand kan worden.
   Voorgestelde maatregelen:
   - Bij inrichting nieuwe werkomgeving goede beveiliging voor externe opslagmedia realiseren. (medio 2011)

3. Stroomstoring en Niet beschikbaar (zijn van het informatiesysteem)
   De gemeente heeft de beschikking over een UPS die zorg draagt dat de servers netjes worden afgesloten. Er is echter geen aggregaat om tijdens een stroomstoring (met minimale middelen) door te werken.
   Er is door burgerzaken een contract gesloten met IBM waarin de uitwijk voor het GBA systeem, eventueel naar locatie Westergracht, is geborgd. Het GWS4all systeem bevindt zich op dezelfde server als waarop het GBA systeem draait. De veronderstelling is dat als er een calamiteit zich voordoet op deze server de volledige server wordt gere-stored. Nergens in de contracten wordt hier echter zekerheid over geboden. Waardoor we tot de volgende conclusie komen; "In strikt formele zin is er ten behoeve van het systeem GWS4all geen uitwijkvoorziening getroffen."
   Voorgestelde maatregelen:
   - Uitbreiden continuïteitsplan met GWS4all
   - In nieuwe vestiging expliciet aandacht besteden aan continuïteit (medio 2011)

4. Interne fraude en ongeautoriseerd gebruik systeem
   Ten aanzien van het ongeautoriseerd gebruik systeem en het uitlekken van vertrouwelijke informatie hebben we te maken met een combinatie van zowel instrumentele als cultuur en gedrags factoren. Ten eerste kunnen we constateren dat de Gemeente Haarlem onvoldoende beveiligingsbewust is.
   Bevoegdheden voor toegang tot Suwinet worden breed toegekend en er is nauwelijks onderscheid in de bevoegdheden van de verschillende functies. Een periodieke beoordeling van de autorisaties door de beveiligingsbeheerder vindt niet plaats.
   De gemeente Haarlem is weinig actief in het opschonen van gebruikersaccounts. De accounts van uitdienst getreden medewerkers worden niet tijdig verwijderd met als gevolg dat ze tot 90 dagen na uitdienst nog actief zijn.
   Voorgestelde maatregelen:
   - Opstellen Procedure uitdiensttreding medewerker. Met name het afmelden van de autorisaties speelt hierbij een belangrijke rol
   - Continue aandacht van medewerkers voor beveiligingsaspecten.

Managementsamenvatting

Beveiliging binnen Sociale Zaken en Werkgelegenheid

Gemeente Haarlem

Inleiding

Een organisatie als de gemeente Haarlem is constant bezig met het vastleggen en beheren van informatie. De gemeente is veelal verantwoordelijk voor de kwaliteit van deze informatie. Kwalitatief goede informatie is informatie die volledig, juist en tijdig beschikbaar wordt gesteld aan medewerkers en (in beperkte mate aan) burgers. Deze informatie kan alleen worden ingezien en aangepast door medewerkers en burgers die daartoe bevoegd zijn en is altijd op te vragen wanneer het noodzakelijk is. Informatiebeveiliging is juist hierop gericht. Niet alleen heeft de gemeente Haarlem zelf een verantwoordelijkheid om de beveiliging van informatie en informatiesystemen adequaat te regelen, ook de wetgever stelt steeds meer eisen als het gaat om informatiebeveiliging. Zo is deze voor Sociale Zaken en Werkgelegenheid vastgelegd in de SUWI regeling. Maar ook in de Wet Bescherming Persoonsgegevens.

Het beheersen van de risico's die samenhangen met informatie en informatiesystemen (informatiebeveiliging) is dus een belangrijk aandachtsgebied. De gemeente Haarlem heeft daarom een project opgezet om het beveiligingsbeleid van de afdeling Sociale Zaken en Werkgelegenheid te formuleren de risico's in kaart te brengen en vervolgstappen te definiëren om een duurzame doch flexibele basis voor de toekomst neer te leggen.

De schade als gevolg van een incidenten/calamiteiten kan aanzienlijk zijn. Denk hierbij aan financiële schade (operationele herstelkosten), schade als gevolg van onrechtmatigheid, mogelijke juridische aansprakelijkheid, imagoschade (negatieve publiciteit) en de mogelijke gevolgen hiervan: maatschappelijke en politieke discussie over de rol van het gemeentelijk bestuur. Voorbeelden van incidenten uit de praktijk zijn de verloren USB-sticks met gevoelige informatie/dossiers bij defensie en politie en de affaire binnen justitie over gegevens op een computer die is weggegooid zonder de gegevens te verwijderen. Om dit soort schade binnen de gemeente Haarlem te beperken is er voor Sociale Zaken en werkgelegenheid een informatiebeveiligingsplan opgesteld.

Implementatie

De gemeente Haarlem heeft een consistente beveiligingsstrategie en betrouwbare processen nodig om op de hoogte te blijven van de laatste ontwikkelingen op het gebied van technologie en bedreigingen. Beveiliging moet worden benaderd vanuit een breed en strategisch perspectief. Zo ontstaat een systeem dat betrouwbaar en integer is, zelfstandig kan werken, data vertrouwelijk houdt en toegankelijk blijft voor de juiste mensen. In het voorliggende beveiligingsplan Sociale Zaken en Wergelegenheid is op een handzame wijze invulling gegeven aan de eisen die vanuit de SUWI regeling aan gemeenten is opgedragen.
Bij het opstellen van het informatiebeveiligingsplan is specifiek gekeken naar de realiseerbaarheid ervan. Het te hoog leggen van de lat kan er namelijk toe leiden dat doelen niet gehaald worden. Het beveiligingsplan gaat daarom uit van een haalbaar doch acceptabel niveau van informatiebeveiliging. Haalbaar wil niet zeggen dat aan alle elementen op korte termijn kan worden voldaan. In de communicatie naar het College/Raad en de ambtelijke organisatie toe is het van belang om aan te geven dat er wordt uitgegaan van een groeipad.

Aanbevelingen informatiebeveiliging

Doormiddel van het uitvoeren van een risico analyse is er een beeld ontstaan over de huidige stand van zaken aangaande het beveiligingsniveau van de gemeente Haarlem.

De belangrijkste conclusies en aanbevelingen die uit deze risico analyse naar voren zijn gekomen zijn de volgende:

Van de meeste bedreigingen kan op grond van de kennis en ervaring van de geïnterviewden worden gesteld dat deze qua kans van optreden en mogelijke schade gering zijn. Toch zijn er een vijftal punten die aandacht believen:

a) Binnen de afdeling Sociale Zaken en Werkgelegenheid van de gemeente Haarlem is er onvoldoende beveiligingsbewustzijn.
b) Er is geen uitwijkvoorziening voor de applicaties van Sociale Zaken en Werkgelegenheid.
c) Er is geen aggregaat op de locatie Zijlsingel aanwezig.
d) Het netwerk van de gemeente Haarlem is te transparant waardoor de mogelijkheid om het netwerk te infecteren met een virus een reële bedreiging vormt.
e) Bij het beheer van bevoegdheden gebruik te maken van Suwinet, overige informatiesystemen van SZW en het gemeentebrede netwerk wordt te weinig aandacht besteed aan het tijdig verwijderen van niet meer actieve accounts. Hiervoor zal een striktere procedure moeten worden ontwikkeld.

ad a) Onvoldoende Beveiligingsbewustzijn
Om ervoor te zorgen dat er geen "papieren tijger" wordt opgeleverd, is het zaak dat er aandacht wordt besteed aan het borgen van informatiebeveiliging in de organisatie. De 'sense of urgency' aangaande het onderwerp beveiliging moet gemeente breed worden gedragen. Bewustwording bij het management is daarom van cruciaal belang voor het uitdragen van het belang van beveiliging. De beveiligingsproblemen zitten niet in de hard- en software maar in het uitdragen van consistent beleid, de vertaling daarvan in duidelijke procedures en de handhaving.
Verantwoordelijke: Management en leidingevenden SZW

ad b) Uitwijk mogelijkheid bij een calamiteit
De afdeling informatievoorziening afdeling zorgt er centraal voor dat gegevens worden veiliggesteld middels back-ups zodat er in het geval van een verstoring teruggevallen kan worden op deze back-up. Echter als de calamiteit een grotere omvang kent, waarbij ook de servers en werkstations niet meer bruikbaar zijn schrijft de SUWI regeling voor dat er binnen 72 uur de dienstverlening weer opgepakt moet kunnen worden. In dit soort gevallen is het dus nodig om over een uitwijkmogelijkheid te beschikken. Momenteel voldoet de gemeente Haarlem niet aan dit criterium voor de afdeling Sociale Zaken en Werkgelegenheid.
Verantwoordelijke: MS/Informatievoorziening i.s.m. SZW

ad c) Storing
In het geval van een stroomstoring wordt er direct overgeschakeld op de UPS die zorg draagt dat alle servers netjes worden afgesloten zodat de data wordt veiliggesteld. Er is echter geen voorziening getroffen die het mogelijk maakt om de systemen weer op te starten op de locatie Zijlsingel. Door het inzetten van een aggregaat kan voorkomen worden dat medewerkers tijdens een dergelijke storing niet kunnen werken. Het verdient daarom aandacht om in de te realiseren nieuwbouw rekening te houden met een dergelijk voorziening. Verantwoordelijke: MS/Informatievoorziening

ad d) Open netwerk
De gemeente Haarlem heeft een "clean desk" beleid vastgesteld voor papieren en verwijderbare opslagmedia en een "clear screen" beleid voor ICT-voorzieningen. Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken. Hiermee is een goede stap gezet in de juiste richting. Echter blijft de kans voor infecties van virussen een reëel gevaar vormen zolang iedere PC een open USB toegang kent.
Verantwoordelijke: MS/Informatievoorziening

ad e) Personele aspecten
Van iedere nieuwe werknemer worden referenties gecontroleerd en wordt eventueel aanvullend om een verklaring omtrent gedrag (VOG) gevraagd en alle nieuwe in dienst tredende medewerkers leggen de ambtseed of -belofte af.
Voor tijdelijk personeel zoals uitzendkrachten, stagiaires en ingehuurde externe personen, is het tekenen van een geheimhoudingsverklaring noodzakelijk. Bij het vervullen van kwetsbare functies kan door de verantwoordelijke manager gekozen worden om een VOG te vragen.
Bij het uitdiensttreden of beeindigen van een opdracht moeten eventuele pasjes en sleutels worden ingeleverd. Evenals dat de autorisaties op de systemen ook moet worden beeindigd. Het is zaak om hier eenduidige afspraken over te maken die voor de gehele gemeente gelden.
Verantwoordelijke: MS/Informatievoorziening en MS/HRM i.s.m. hoofdafdelingen.

ICT beveiliging
Steeds meer informatie wordt digitaal opgeslagen en over niet al te lange tijd zal deze in papieren vorm zelfs grotendeels verdwijnen van de werkplek. Denk aan ontwikkelingen op het gebied van gedigitaliseerde werkprocessen in combinatie met het scannen van documenten.
Vanuit de afdeling informatievoorziening wordt in samenwerking met de gegevenseigenaren ervoor zorg gedragen dat de mate van informatiebeveiliging wordt aangepast aan de gevoeligheid van de gegevens. Op het gebied van privacy zit er een verschil in de gegevens die voor beoordeling van een uitkering nodig zijn en de financiële administratie.
De afdeling informatievoorziening zorgt er centraal voor dat gegevens worden veiliggesteld (back-ups) en dat in het geval van een calamiteit kan worden uitgeweken. De gegevenseigenaren zijn er vervolgens zelf weer voor verantwoordelijk voor om de overige zaken te regelen.

Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid

Gemeente Haarlem

Versie : 1.0
Status : definitief
Auteur : de heer M. van Schoonhoven
Proces verantwoordelijke : de heer R.J.A. van Noort
Datum : 30 juni 2010
Bestuur en Management Consultants (BMC)

Inhoudsopgave

1. Algemeen

1.1. Inleiding

In de gemeentelijke organisatie is een toenemend gebruik van geautomatiseerde informatiesystemen te constateren. Over 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. Voorliggende Basis beveiligingsrichtlijnen zijn 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 deze Basis beveiligingsrichtlijnen zijn de uitgangspunten en beveiligingsprocedures opgenomen, welke invulling geven aan al deze eisen.

1.2. Regeling SUWI

Doelstellingen en taken van de Hoofdafdeling Sociale zaken en Werkgelegenheid vloeien voort uit de Regeling SUWI (Wet van 29 november 2001). Dit betreft met name de processen rond Sociale Zaken en Werkgelegenheid. Met deze processen worden persoonsgegevens geadministreerd en verwerkt. Ook vindt gegevensuitwisseling plaats met de SUWI-partners, zoals het UWV en UWV Werkbedrijf.

1.3. WBP / Bijlage XIV

Uitgangspunt van de informatiebeveiliging voor de verwerking van de persoonsgegevens is de Wet Bescherming Persoonsgegevens. Bijlage XIV van de Regeling SUWI schrijft voor aan welke eisen de beveiligingsfunctie moet voldoen en volgens welke normen deze moet zijn ingericht en werken.
SUWI-net partijen geven op basis van artikel 6.4 uit de Regeling SUWI in een beveiligingsplan aan op welke wijze zij invulling geven aan het de beveiliging van de gegevensuitwisseling tegen inbreuken op de beschikbaarheid, de data integriteit en de vertrouwelijkheid. Overeenkomstig hetgeen in de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald (zie Richtlijnenboek informatiebeveiliging SUWI gemeenten).

1.4. 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 de Basis beveiligingsrichtlijnen staat beschreven.
Voor accordering van de Basis beveiligingsrichtlijnen tekent hieronder de opdrachtgever:

Gemeente Haarlem
College van B&W
Postbus 511
2003 PB Haarlem

Burgemeester, de heer B.B. Schneiders

Plaats en datum: Haarlem, 30 juni 2010

Handtekening:

Gemeentesecretaris, mevrouw S. Borgers

Plaats en datum: Haarlem, 30 juni 2010

Handtekening:

2. Versiebeheer

Versie	Datum	Auteur	Status	Aard wijzigingen	Verstuurd aan
0.1	7 april 2010	de heer M. van Schoonhoven	concept	1e concept	Beveiligingswerkgroep
0.2	14 juni 2010	de heer M. van Schoonhoven	concept	2e concept	Beveiligingswerkgroep
1.0	30 juni 2010	de heer M. van Schoonhoven	Concept	3e concept	W. Mevissen
1.1	30 augustus 2010	de heer M. van Schoonhoven	Definitief	Finale	W. Mevissen

2.1. Werkgroep informatiebeveiliging Sociale Zaken en werkgelegenheid

Ten behoeve van de totstandkoming van en periodieke afstemming (minimaal tweemaal per jaar) over voorliggend Informatiebeveiligingsplan is door de gemeente Haarlem een (permanent) Werkgroep informatiebeveiliging Sociale Zaken en werkgelegenheid ingesteld.

Deze Werkgroep informatiebeveiliging Sociale Zaken en werkgelegenheid Bestaat uit de volgende medewerkers:

- Marco van Schoonhoven (BMC)
- Rob Corzilius (Afdelingshoofd SZW/Werk en Inkomen B)
- Angelica vd Kraan, coörd. informatiebeveiliging SZW (Medew. kwaliteitszorg, SZW/BB)
- Joep Kint (Coörd. applicatiebeheer SZW/BB)
- Theo Bleeker, netwerkbeheerder (Technisch beheerder MS/IV/IS)
- Willy Mevissen, beveiligingscoördinator a.i. (beleidsmedewerker informatievoorziening (MS/IV/IB)

2.2. Verantwoording

Voorliggende Basis beveiligingsrichtlijnen zijn gebaseerd op de normen[1] zoals vastgesteld in de eisen van het ministerie. Deze eisen zijn gebaseerd op de continuïteitseisen zoals beschreven in de 'Code voor Informatiebeveiliging' (ISO 27002)[2].

[1] Zie verificatielijst SUWI-normen

[2] Zie voor korte toelichting bijlage I 'Toelichting ISO 27002'

2.3. 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 beveiligingscoördinator worden vastgesteld of de maatregelen worden nageleefd. Verder verdient het aanbeveling minimaal eenmaal per jaar het beleid te evalueren en eventueel te herzien.
De voorliggende Basis beveiligingsrichtlijnen bevatten tevens een stelsel van procedures en maatregelen voor de dagelijkse praktijk. Dit stelsel moet regelmatig worden bezien op actualiteit. In de Basis beveiligingsrichtlijnen 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 document Basis beveiligingsrichtlijnen 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 4 'Functieverdeling SUWI'. Daarnaast dient het gehele beleid minimaal eenmaal per raadsperiode te worden herijkt.

3. Beveiliging

3.1. 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. Vanuit de SUWI regelgeving zijn normen gedefinieerd. De gemeente moet in het kader van de Wet SUWI "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.

3.2. 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.
In het kader van de SUWI worden ten aanzien van de vertrouwelijkheid, data integriteit (juistheid, volledigheid en tijdigheid) en continuïteit 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 vertrouwelijkheid, data integriteit en continuïteit, 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.

3.3. 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 en diskette Communicatieapparatuur.
- Supplies als tapes, Cd's, en DVD's.

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 AIX en Novell een (respons) onderhoudscontract afgesloten door de gemeente Haarlem. Zie hiervoor de Bijlage 13 ´Onderhoudscontract SUWI´.
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 geen uitwijkcontract afgesloten voor de applicaties van Sociale Zaken en Werkgegenheid.

3.4. 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 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 Basis beveiligingsrichtlijnen op AIX en Novell de applicatie GWS4all van de leverancier Centric.

3.5. 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. In procedure 6 'Continuïteitsbeheer' wordt nader ingegaan op het uitvoeren van de back-up in Haarlem.

3.5.1. Classificatie van informatie en bedrijfsmiddelen

In deze paragraaf wordt aangegeven op welke wijze informatie binnen het SUWI domein is gecategoriseerd. Binnen de Gemeente Haarlem wordt gewerkt met persoonsgegevens die aangemerkt kunnen worden als bijzondere persoonsgegevens zoals beschreven in artikel 16 Wet Bescherming Persoonsgegevens. Omdat deze gegevens niet specifiek onderscheiden kunnen worden binnen de gegevensuitwisseling en gezien het grote aantal uitwisselingen, wordt de risicoklasse[3] van de gegevens vastgesteld op een combinatie van II en III.

Logbestanden en de gebruikersadministratie bevatten persoonsgegevens van medewerkers. De gegevens die worden vastgelegd in deze bestanden worden vastgelegd in risicoklasse I. Door middel van GWS4all en digitale dossiers zijn verschillende soorten gegevens gecategoriseerd. Om te voorkomen dat medewerkers van de dienst bij een eventuele crash van het netwerk gegevens voor langere tijd kwijt zijn, worden dagelijks back-ups gedraaid van alle servers. Concreet betekent dit dat alle gegevens die zich op de servers bevinden (data, rapporten, beschikkingen etc) elke avond worden opgeslagen. Het feitelijk uitvoeren van de back-ups wordt uitgevoerd door de afdeling informatievoorziening. Binnen de gemeente is afgesproken dat slechts medewerkers die werkzaam zijn in het primaire proces en de sociale rechercheurs toegang krijgen tot SUWI-net en GWS4all en wordt alleen voor hen een gebruikersaccount en wachtwoord aangemaakt. Wachtwoorden zijn strikt persoonlijk en mogen niet worden overgedragen. Naast inloggen op het gemeentelijk netwerk is een aparte inlogactie noodzakelijk voor SUWI-net en GWS4all.

3.6. Datacommunicatie verbindingen

Onder verbindingen worden verstaan de communicatielijnen die verschillende computers onderling met elkaar verbinden. Vooral zodra het openbare kabelnetwerk of telefoonnet als communicatiemedium wordt gebruikt loopt men het risico dat onbevoegden het informatiesysteem binnendringen. Voor hackers gaat op dit punt echt geen berg 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 van Sophos. Zie hiervoor ook de Procedure 2 'Antivirus voorzieningen SUWI'.

3 Zie Bijlage II Risicoklasse Bron: 'Richtlijnenboek Informatiebeveiliging SUWI gemeenten – GSD'

3.7. Documentatie

Onder documentatie wordt verstaan:

3.7.1. 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.

3.7.2. 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 hoofd van de afdeling ICT. De verantwoordelijkheid voor het bijhouden van de gebruikersdocumentatie ligt bij de functioneel applicatiebeheerder.

3.8. Het gebouw

De Locatie Zijlzingel in Haarlem is op een aantal manieren beveiligd. Er zijn voorzieningen getroffen ten behoeve van de fysieke beveiliging door de firma NVD uit Haarlem. Hierbij is sprake van compartimentering van het gebouw. Tevens is er een inbraakwerende voorziening (stil alarm naar de meldcentrale van NVD).
De zogenoemde kritische ruimten zijn afgesloten voor het publiek. In een gedeelte van het stadhuis zijn inbraakwerende voorzieningen getroffen in de vorm van bewegingsmelders. Er is een elektronische toegangsbeveiliging voor het stadhuis. 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.

3.8.1. Fysieke beveiliging dislocaties

Er zijn binnen de gemeente Haarlem diverse dislocatie waar gebruik gemaakt kan worden van GWS4all en SUWI inkijk. In Bijlage 18 Aansluitingen op gemeentelijk netwerk Haarlem zijn alle dislocaties benoemd waarvoor dit geldt.

3.8.2. 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:

- Kluis Brinkmann.
- Computerruimte.
- Werkruimten.

3.9. 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.

3.10. Clean desk en clear screen beleid

De Gemeente Haarlem stelt een "clean desk" beleid vast voor papieren en verwijderbare opslagmedia en een "clear screen" beleid voor ICT voorzieningen. Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken. Hierin wordt rekening gehouden met de classificatie van informatie en bedrijfsmiddelen (zie 4.2).

In dit beleid komen onderstaande punten aan de orde:

- Bij het (tijdelijk) verlaten van de werkplek wordt vertrouwelijke, privacygevoelige en/of kritische informatie opgeborgen en wordt de werkplek, indien mogelijk, afgesloten.
- Vertrouwelijke en/of privacygevoelige informatie wordt bewaard in een deugdelijk af te sluiten (waarde)kast of kluis.
- Werkstations en Thin Clients mogen niet toegankelijk zijn voor onbevoegden wanneer zij onbeheerd achterblijven. (bij geen gebruik worden de werkstation automatisch na 10 minuten vergrendeld).
- Vertrouwelijke en/of privacygevoelige informatie wordt na het afdrukken onmiddellijk van de printer verwijderd.

4. Waar tegen moet worden beveiligd?

4.1. 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 SUWI 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.

4.2. 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 gedurende welke 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 SUWI moet de beschikbaarheid van de dienstverlening worden verzekerd naar de burger, de interne afnemers en de externe afnemers. Gestreefd moet worden naar een optimale continuïteit. Dit maakt een uitwijkvoorziening noodzakelijk.

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.

5. Informatiebeveiligingsbeleid

5.1. 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 continuïteit, 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.

5.2. Sectorale wet- en regelgeving

Ook in de sectorale wetgeving zijn bepalingen opgenomen die tot doel hebben de persoonlijke levenssfeer van betrokkenen te beschermen. De sectorale wet- en regelgeving die relevant is voor de Hoofdafdeling Sociale zaken en Werkgelegenheid en voor de samenwerking in SUWI-verband betreft de SUWI regelgeving: de Wet Structuur uitvoering werk en inkomen (wet SUWI), het Besluit en de Regeling SUWI.

5.2.1. SUWI

Uit de SUWI regelgeving vloeien doel en taken van de Hoofdafdeling Sociale zaken en Werkgelegenheid en de overige SUWI- organisaties voort. De sectorale wetgeving regelt onder meer de informatievoorziening van de SUWI- organisaties onderling en aan derden. Daarbij is bepaald dat de gegevensstromen tussen de SUWI- organisaties via het SUWI-net verlopen. Gegevensstromen waarin de SUWI regelgeving niet voorziet zal, zonder goedkeuring van de Minister, niet plaatsvinden. Voor zover in de wet SUWI niet van de WBP wordt afgeweken, geldt de WBP.
Vanaf invoering van SUWI dient iedere gemeente overeenkomstig Artikel 6.4, Regeling SUWI, in een beveiligingsplan aan te geven op welke wijze zij invulling geeft aan de beveiliging van de gegevensuitwisseling in het kader van de wet SUWI. In het Verslag over de uitvoering WWB rapporteert de gemeente ieder jaar of zij voldoet aan de beveiligingseisen die als SUWI-net partij aan hen worden gesteld vanuit bijlage XIV Regeling SUWI. In deze bijlage wordt er gevraagd of er een actueel beveiligingsplan aanwezig is bij de gemeente. In het verantwoordingsverslag (onderdeel 2B, de kwalitatieve rechtmatigheidsonderdelen) hoeft alleen iets te worden ingevuld als er een tekortkoming in de beveiliging wordt geconstateerd. (zie ook: Handleiding, Bijlage K: Verantwoording). Het Richtlijnenboek informatiebeveiliging SUWI gemeenten kunt u beschouwen als een 1 op 1 vertaling van bijlage XIV van de Regeling SUWI.

5.2.2. WWB

Daarnaast zijn de Wet Werk en Bijstand (WWB) en aanverwante wetgeving relevant. In de WWB is een aparte paragraaf opgenomen over de regels die van toepassing zijn bij de uitwisseling van persoonsgegevens. Deze paragraaf kan als volgt op hoofdlijnen worden geschetst:
Werkgevers hebben een informatieplicht om inlichtingen te verstrekken aan de Hoofdafdeling Sociale zaken en Werkgelegenheid omtrent de aanvrager van een uitkering of een uitkeringsgerechtigde betreffende omstandigheden die noodzakelijk zijn voor de uitvoering van de WWB;
Diverse instanties, zoals de UWV Werkbedrijf, het UWV, overige gemeenten, College voor zorgverzekeringen, pensioenfondsen, etc. hebben een informatieplicht naar de Hoofdafdeling Sociale zaken en Werkgelegenheid indien noodzakelijk voor de uitvoering van de WWB;
Medewerkers die met persoonsgegevens in aanraking komen hebben een geheimhoudingsplicht, tenzij het voor de uitvoering van de WWB noodzakelijk is deze persoonsgegevens te verstrekken.
De gemeente heeft een inlichtingenverplichting binnen gestelde regels ten aanzien van diverse instellingen, zoals de UWV Werkbedrijf, het UWV, de Sociale Verzekeringsbank, de Belastingdienst, overige gemeenten etc. Voor de verstrekking van gegevens tussen instanties wordt gebruik gemaakt van het Burger Service Nummer (BSN).
Via het verslag over de uitvoering WWB dient de gemeente zich ook te verantwoorden over de juiste naleving van de WWB-bepalingen die betrekking hebben op gegevensuitwisseling.

5.2.3. Overige wetgeving

Naast de sectorale wet- en regelgeving en de WBP gelden er diverse andere wet- en regelgevingen, zoals de Wet voor Computercriminaliteit, de Auteurswet en de Archiefwet. Vanwege het algemene karakter van dit voorliggende beleid wordt hier verder niet op ingegaan en wordt e.e.a. overgelaten aan de Hoofdafdeling Sociale zaken en Werkgelegenheid.

5.3. Fysieke beveiliging

Volgens de inleiding EDP-auditing[4] 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 welke 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 Basis beveiligingsrichtlijnen is in hoofdstuk 3 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.

[4] 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 beschreven in bijlage 14 ´Risico-inventarisatie en evaluatie Informatiebeveiliging SUWI´.

5.4. Informatiebeveiliging

Informatiebeveiligingsbeleid is volgens de Code voor Informatiebeveiliging[5] het op schrift gesteld en door het gemeentebestuur en het directieteam 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 het directieteam 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 continuïteit, vertrouwelijkheid en data 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%.

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 het directieteam met betrekking tot informatiebeveiliging.

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

Ad 5) Dit document wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld door de beveiligingscoördinator 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.

[5] 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.

5.5. Beveiligingseisen ten aanzien van personeel

5.5.1. Beveiligingseisen bij aanname van personeel

Door middel van deze paragraaf wordt in kaart gebracht op welke manier de gemeente aandacht schenkt aan informatiebeveiliging ten aanzien van personeel.

Vast personeel
Personeel dat in dienst is bij de gemeente valt direct onder het ambtenarenreglement. Dit betekent dat zij bij benoeming niet apart een verklaring dienen te ondertekenen dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In het ambtenarenreglement is dit reeds opgenomen. Wel krijgen medewerkers na hun benoeming een gemeentebrede introductie. Tijdens deze introductie wordt de ambtseed afgenomen. Als ambtenaar verplicht je jezelf dan alle zaken waarvan je weet of vermoedt dat ze een vertrouwelijk karakter hebben, geheim te houden.

Tijdelijk personeel
Personeel dat werkzaamheden verricht bij de gemeente en niet in een ambtelijk dienstverband is benoemd, wordt bij het aangaan van het tijdelijke dienstverband, gevraagd een verklaring tekenen dat volgens de gestelde eisen omgegaan wordt met privacygevoelige informatie.

Bij aanname van personeel worden de behaalde diploma's overlegd, waarna deze worden opgeborgen in het personeelsdossier. Ook dienen medewerkers ingevolge de Wet op de Identificatieplicht bij aanname een kopie van hun legitimatiebewijs te overleggen. Medewerkers tekenen geen aparte geheimhoudingsverklaring.

5.5.2. Training voor gebruikers

De afdeling Sociale Zaken en Werkgelegenheid instrueert de individuele gebruikers over correcte omgang met ICT-voorzieningen. In deze paragraaf wordt dit summier aangegeven.
Binnen de afdeling Sociale Zaken en Werkgelegenheid wordt met betrekking tot SUWI-net en GWS4all een gebruikershandleiding verzonden aan alle nieuwe gebruikers.
Tijdens de algemene introductie van nieuwe medewerkers worden zij in kennis gesteld van het gebruik van privacygevoelige informatie.
Er zijn voor SUWI-net en GWS4all handreikingen opgesteld in welke situatie al dan niet informatie aan klanten en/of derden verstrekt mag worden.

5.6. Raakvlakken met ander beleid

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

5.7. Taken, verantwoordelijkheden en bevoegdheden

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

Voor alle in de Basis beveiligingsrichtlijnen voorkomende functies is in Bijlage 4 ´Functieverdeling SUWI´ de vervanging vastgelegd.

5.7.1. 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 deze Basis beveiligingsrichtlijnen vast. Het college van B&W onderschrijft volledig de beveiligingsmaatregelen die in de Basis beveiligingsrichtlijnen 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 regelingen Werk en Inkomen.

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

5.7.2. Verantwoordelijkheden van het directieteam

Beveiliging is op ambtelijk niveau de verantwoordelijkheid van alle leden van het directieteam van de gemeente Haarlem. Het directieteam 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 Basis beveiligingsrichtlijnen en gerapporteerd door de beveiligingscoördinator.
- Mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen.
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de beveiligingscoördinator.
- 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.

5.7.3. Verantwoordelijkheden van de beveiligingscoördinator

Door het college van B&W is de beveiligingscoördinator in de rol van beveiligingsbeheerder SUWI benoemd (verder genoemd de intern controleur). De beveiligingscoördinator is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Basis beveiligingsrichtlijnen SUWI. De beveiligingscoördinator rapporteert periodiek (minimaal eens per jaar) aan het college van B&W en het directieteam, zo nodig zonder tussenkomst van de diverse afdelingsmanagers.
Onder beveiligingscoördinator 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 beveiligingscoördinator 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 het directieteam.
- 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 beveiligingscoördinator verstrekt daarnaast gevraagd en ongevraagd adviezen om te komen tot het gewenste beveiligingsniveau.

5.8. 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 SUWI 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 SUWI: de gegevens die worden verwerkt hebben betrekking op een deel van de bevolking van de gemeente Haarlem.

Risicoklasse II
Bij onderhoud aan apparatuur door derden moet de vertrouwelijke omgang met persoonsgegevens in het contract zijn vastgelegd. De toegankelijkheid van de persoonsgegevens door derden moet zo veel mogelijk beperkt zijn. Voor het testen van informatiesystemen met persoonsgegevens mogen uitsluitend gegevens van fictieve personen gebruikt worden.

1. *Bron : Bureau Keteninformatisering Werk en Inkomen Richtlijn gebruik productiegegevens*

5.8.1. 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 welke 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.

5.8.2. Kwaliteitsaspecten

Informatiebeveiligingsbeleid is niets anders dan een verzameling van strategische uitgangspunten waarin de bestuurlijke en ambtelijk top duidelijk maakt 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: **continuïteit**	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: **data-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 controleerbaarheid. 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:

5.8.3. Norm voor continuïteit

Het College van B&W en het directieteam 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 SUWI applicatie.

De openingstijden (voor het publiek) zijn:

Maandag - vrijdag van 9.00 tot 16.00 uur, donderdag van 9.00 tot 20.00 uur.

Daarnaast dient de informatievoorziening rondom GWS4all op jaarbasis tijdens kantooruren voor 99,82% beschikbaar te zijn (dat is ongeveer 4 uur aan verstoringen per jaar).

Als kantooruren worden hier bedoeld: Maandag - vrijdag van 7.30 tot 19.00 uur, donderdag van 7.30 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 SUWI-netwerk) te kunnen voortzetten.

5.8.4. Norm voor data 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.

5.8.5. 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 SUWI gegevens in aanraking komen dienen de ambtseed te hebben afgelegd dan wel een verklaring te hebben ondertekend.
Alle meldingen van verwerkingen van persoonsgegevens die in de zin van de regeling SUWI en de Wet Bescherming Persoonsgegevens verplicht zijn, zijn door de gemeente gedaan aan het College Bescherming Persoonsgegevens in Den Haag.

5.8.6. 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.

6. Beveiligingsincidenten

6.1. Aanpak incidenten en zwakke plekken

Incidenten waarbij de vertrouwelijkheid, data integriteit of continuïteit van Sociale Zaken en Werkgelegenheid in het geding zijn, worden afgehandeld als beveiligingsincident. Incidenten en zwakke plekken in de beveiliging kunnen op diverse manieren worden ontdekt:

- Bij toeval, door een gebruiker, beheerder of helpdeskmedewerker;
- Als uitkomst van gericht onderzoek naar incidenten en/of zwakke plekken vanuit reguliere (beheer)werkzaamheden. Hierbij kan worden gedacht aan virusscanning, monitoring en analyse van logbestanden/rapportages.
- Als uitkomst van een specifiek onderzoek. Hierbij kan worden gedacht aan een beveiligingsaudit of een onderzoek naar aanleiding van nieuwe bedreigingen (bekend geworden zwakke plekken in besturingssystemen, nieuwe virussen etc).

6.2. Mogelijke incidenten

Incidenten zijn die gebeurtenissen die schade kunnen veroorzaken aan de vertrouwelijkheid, data integriteit of beschikbaarheid van informatie of informatieverwerking. Zij openbaren zich als een al dan niet opzettelijke inbreuk op de privacy- of beveiliging van informatie(systemen).

Mogelijke privacy- of beveiligingsincidenten die de vertrouwelijkheid aan kunnen tasten:

- Incidenten die ongeautoriseerde toegang tot informatie mogelijk maken.
- Verlies van gegevensdragers waar vertrouwelijke informatie op staat
- Verlies of diefstal van een laptop.
- Poging van medewerkers om een 'hogere' autorisatie te krijgen buiten de geldende procedures.
- Pogingen van binnenuit of van buitenaf om onrechtmatige toegang te verkrijgen tot systemen (hacken).

Mogelijke incidenten die de data integriteit aan kunnen tasten:

- Dataverlies of het onvolledig verwerken van transacties.
- Slechte tracks op harddisks, fouten in het geheugen.
- Mogelijke pivacy- en beveiligingsincidenten die de beschikbaarheid aan kunnen tasten:
- Een onderbreking van de ICT- dienstverlening voor een onacceptabele periode.
- Virussen, Trojan horses (kwaadaardige software).
- Diefstal van laptops, onderdelen of gegevensdragers.

6.3. Incidentmelding

De ontdekker van het incident meldt het incident, conform procedure 9 'Incidentenbeheer SUWI', aan de beveiligingsmedewerker van zijn vestiging of aan de eigen lijnmanager die het vervolgens meldt aan de betreffende beveiligingsmedewerker. Deze melding wordt vervolgens doorgestuurd naar de beveiligingscoördinator.

6.4. Afhandeling

6.4.1. Aard van de maatregelen

In geval van een beveiligingsincident wordt gestreefd naar een herstel van het gewenste beveiligingsniveau op zo kort mogelijke termijn. In eerste instantie is het streven beveiligingsincidenten te voorkomen (preventie), dan wel de schade ten gevolgen van een eventueel incident bij voorbaat te beperken (repressie). Indien zich een incident voordoet, dient dit tijdig te worden geconstateerd (detectie) en de negatieve consequenties moeten teniet worden gedaan (correctie).

6.4.2. Afsluiting na incident

Wanneer volgens de beveiligingsmedewerker uit onderzoek blijkt dat het beveiligingsincident een ernstige bedreiging vormt voor de beveiliging van het Sociale Zaken en Werkgelegenheid- of SUWI-netwerk, zal hij terstond in overleg treden met de betrokken beheerorganisatie van het Sociale Zaken en Werkgelegenheid- of SUWI-netwerk. Aan de hand van vooraf vastgestelde criteria, kan de beveiligingsmedewerker (in overleg met het management) opdracht geven tot afsluiting van het bedreigde onderdeel van het Sociale Zaken en Werkgelegenheid- of SUWI-netwerk. Herstel van de aansluiting zal plaatsvinden zodra het gewenste beveiligingsniveau van het Sociale Zaken en Werkgelegenheid- of SUWI -netwerk weer gewaarborgd is, zulks ter beoordeling van de beveiligingsmedewerker. Vervolgens vindt in het overleg van de beveiligingsmedewerker en de lijnmanager een evaluatie plaats van de gebeurtenis.

6.5. Rapportage

Alle beveiligingsincidenten worden schriftelijk door de beveiligingsmedewerker aan de lijnmanager en aan de beveiligingscoördinator gerapporteerd met vermelding van de volgende gegevens:

- omschrijving van het incident;
- classificatie van het incident;
- datum en tijdstip van de constatering;
- ondernomen actie om het incident op te heffen (indien mogelijk);
- datum en tijdstip ondernomen actie.

De beveiligingscoördinator rapporteert minimaal één keer per jaar (doch voor 15 maart van het volgende jaar) de SUWI-net specifieke incidenten, via de lijnmanager, aan het Bureau Keteninformatisering Werk en Inkomen (BKWI).

6.6. Zwakke plekken in de beveiliging

Gebruikers dienen (mogelijke) zwakke plekken in de beveiliging te melden aan de beveiligingsmedewerker van de eigen vestiging of aan de eigen lijnmanager die het vervolgens meldt aan de betreffende beveiligingsmedewerker. De beveiligingsmedewerker rapporteert de daadwerkelijk vastgestelde zwakke plek aan de lijnmanager en de beveiligingscoördinator, met vermelding van de volgende gegevens:

- Meldingsgegevens
- Omschrijving van de zwakke plek;
- Inschatting van de impact van de zwakke plek;
- Classificatie van de zwakke plek;
- Datum en tijdstip van de constatering;
- Ondernomen actie om zwakke plek op te heffen (indien mogelijk);
- Datum en tijdstip ondernomen actie.

6.7. Disciplinaire maatregelen

6.7.1. Overtreding door medewerker

In het geval dat een medewerker afwijkt van het beveiligingsbeleid dan wel activiteiten verricht die afbreuk doen aan dit beleid, bestaat voor het verantwoordelijke lijnmanagement de mogelijkheid disciplinaire maatregelen te treffen jegens de betreffende medewerker. De disciplinaire maatregelen zijn gericht op het voorkomen van herhaling van de overtreding en dienen redelijkerwijs in verhouding te staan tot de mate van overtreding. Overtreding van regels kan leiden tot schorsing en/of ontslag op staande voet (bijv. in geval van openbaar maken bedrijfsgeheimen). De mogelijkheid tot het treffen van disciplinaire maatregelen, geldt in gelijke mate voor ingehuurde medewerkers, het geen is vastgelegd in het contract dat met de betreffende partij is afgesloten.

7. Naleving

7.1. Naleving van wettelijke voorschriften

In deze paragraaf wordt de link gelegd tussen informatiebeveiliging en wetgeving.
De gemeente heeft op verschillende onderdelen te maken met wetgeving waar zij aan moet voldoen. Zaken die te maken hebben met de Wet Bescherming Persoonsgegevens, Archiefwet en Wet SUWI zijn beschikbaar in het algemene archief.

De afdeling Sociale Zaken maakt gebruik van verschillende applicaties. Er kan een onderscheid gemaakt worden tussen applicaties die enkel gebruikt worden door onze dienst en applicaties die gemeentebreed worden gebruikt.

- *GWS4all (back office applicatie voor de registratie van uitkeringsgerechtigde* en de daarbij behorende processen)
- *SUWI-Inkijk (webportal waar in SUWI partners gegevens bijhouden van klanten, deze portal wordt gehost door het Inlichtingen bureau).*
- *Key2Burgerzaken (back office applicatie voor de registratie van alle personen binnen de gemeenten en de daarbij behorende processen)*

De informatie inzake de overige applicaties wordt centraal via de Afdeling Informatievoorziening geregistreerd en gedocumenteerd.

7.1.1. Beoordeling van de naleving van het beveiligingsbeleid en de technische vereisten

Binnen de gemeente is een protocol van kracht waarin medewerkers op de hoogte gesteld worden van de richtlijnen hoe om te gaan met internetgebruik. Dit protocol is voor iedere medewerker toegankelijk.

7.1.2. Overwegingen ten aanzien van systeemaudits

Het samenwerkingsverband Audit Aanpak van het College Bescherming Persoonsgegevens (CBP) en diverse instanties hebben auditproducten ontwikkeld waarmee vastgesteld kan worden hoe de sociale dienst persoonsgegevens verwerkt. Deze producten zijn:

- De Quickscan: een beknopte vragenlijst waarmee functionarissen binnen een organisatie snel inzicht kunnen verkrijgen in de mate waarin men zich bewust is van de stand van zaken rond de bescherming persoonsgegevens;
- De WBP Zelfevaluatie: hiermee kan een organisatie zelfstandig en in betrekkelijk korte tijd de kwaliteit van maatregelen voor de bescherming en beveiliging van persoonsgegevens beoordelen. Door bij de uitvoering van de WBP Zelfevaluatie expliciet de sterke punten en verbeterpunten te identificeren, kan een goede basis worden gelegd voor vervolgactiviteiten;
- Binnen de gemeente zal jaarlijks een interne meting plaatsvinden inzake de beveiliging van persoonsgegevens. Deze meting zal verricht worden door de beveiligingscoördinator die tevens in de rol van beveiligingsbeheerder voor SUWI-net is benoemd.

Overzicht Procedures, Rapportage & bijlage Basis beveiligingsrichtlijnen SUWI

Procedure

1. Procedure Herstel van mutaties applicaties Sociale Zaken
2. Procedure Antivirus voorzieningen SUWI
3. Procedure Autorisatie
4. Procedure Autorisatie tot Suwinet-DKD
5. Procedure Communicatie over beveiliging SUWI
6. Procedure Continuïteitsbeheer
7. Procedure gegevensverwerking applicatie Sociale Zaken
8. Procedure Goedkeuren updates applicatie SUWI
9. Procedure Incidentenbeheer SUWI
10. Procedure Instellen en opvragen auditlog
11. Procedure Probleembeheer SUWI
12. Procedure Rapportage van incidenten SUWI
14. Procedure Terugmeldingen en Correctieverzoeken DKD
15. Procedure Vernietiging van verwijderbare media SUWI
16. Procedure Wijzigingenbeheer SUWI

Rapportage

1. Rapportage Controle autorisaties Sociale Zaken
2. Rapportage Controle Terugmeldingen en Correctieverzoeken DKD
3. Rapportage Evaluatie beveiligingsbeleid en plan
4. Rapportage Test reconstructie Sociale Zaken
5. Rapportage Test restore applicatie Sociale Zaken
6. Rapportage Test uitwijk SUWI
7. Rapportage Controle gegevensverwerking SUWI

Bijlage

1. Bijlage Back-up registratie SUWI
2. Bijlage Beheerregeling Sociale Zaken
3. Bijlage Formulier Autorisaties
4. Bijlage Functieverdeling SUWI
5. Bijlage Handreiking autorisatie Suwinet-inkijk
6. Bijlage Intern uitwijkplan geautomatiseerde systemen
7. Bijlage Kenmerken applicaties Sociale Zaken
8. Bijlage Kenmerken computerruimte
9. Bijlage Kenmerken fysieke beveiliging
10. Bijlage Kenmerken Gemeentelijke LAN SUWI
11. Bijlage Kenmerken SUWI applicatie
12. Bijlage Kenmerken SUWI systeem
13. Bijlage Onderhoudscontract SUWI
14. Bijlage Risico-inventarisatie en evaluatie Informatiebeveiliging SUWI
15. Bijlage Verklarende woordenlijst
17. Bijlage Activiteitenkalender informatiebeveiliging
18. Bijlage Aansluitingen op gemeentelijk netwerk Haarlem

Eigen documenten

1. Eigen document 20100208 autorisatie_medewerker GWS_Liaan__1
2. Eigen document Autorisatie GBA Nieuwe medewerker
3. Eigen document Autorisatie Nieuwe netwerkgebruiker
4. Eigen document Geheimhoudingsverkaring Nieuwe medewerker
5. Eigen document HANDLEIDING versie 6 van intranet
6. Eigen document Instructie Autorisaties - Intranet

Bijlage II Risicoklasse

Informatiebeveiliging en privacy

Informatiebeveiliging is voor de Hoofdafdeling Sociale zaken en Werkgelegenheid van essentieel belang en behoort een onderdeel te zijn van de dagelijkse werkzaamheden van managers en medewerkers. In het kader van de uitwisseling van gegevens met andere Suwi-organisaties wordt aan de beveiliging hiervan een aantal eisen gesteld. De daadwerkelijke beveiligingsmaatregelen rond de gegevensuitwisseling via Suwi-net moeten bij alle organisaties van een gelijkwaardig niveau zijn en niet sterk van elkaar afwijken.

Ook vanuit de wetgeving wordt aan de uitwisseling van gegevens een aantal eisen gesteld. Zo is op 1 september 2001 de nieuwe Wet Bescherming Persoonsgegevens (WBP) in werking getreden. Deze wet bevat een grote hoeveelheid regels voor het bewaren, inzien, raadplegen, verstrekken, koppelen, archiveren, kopiëren en vernietigen van gegevens. Al deze vormen van "verwerken" moeten in overeenstemming met de wet en behoorlijk en zorgvuldig plaatsvinden (artikel 7 WBP) en zijn slechts toegestaan op basis van een of meer in de WBP genoemde grondslagen (artikel 8 WBP).

Op grond van de WBP kan een cliënt bij de Hoofdafdeling Sociale zaken en Werkgelegenheid inzage vragen in of correctie vragen van gegevens. Zulke verzoeken vereisen een zorgvuldige behandeling. Datzelfde geldt, in nog sterkere mate, bij de verstrekking van gegevens aan derden. Naast deze privacyaspecten van de gegevensuitwisseling dienen ook algemene beveiligingsaspecten in acht te worden genomen. In artikel 13 WBP is namelijk bepaald dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de 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 gegevens met zich brengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De vraag welke beveiligingsmaatregelen door gemeenten c.q. de Hoofdafdeling Sociale zaken en Werkgelegenheid moeten worden genomen in het kader van de gegevensuitwisseling die plaatsvindt via het Suwi-net dient te worden beantwoord aan de hand van de maatregelen omschreven in de zogenaamde risicoklassen. Het CBP gaat in haar rapport "Beveiliging van persoonsgegevens, achtergrondstudies en verkenningen 23" uit van de navolgende vier risicoklassen:

- Risicoklasse 0 publiek niveau;
- Risicoklasse I basis niveau;
- Risicoklasse II verhoogd risico;
- Risicoklasse III hoog risico.

In bijlage XIV van de Regeling SUWI wordt bepaald dat de gegevensuitwisseling die plaatsvindt binnen Suwi-net onder te brengen is in de risicoklasse II/III.

Risicoklasse 0: Publiek niveau
Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites etc. De persoonsgegevens behoeven ten aanzien van de exclusiviteit van de persoonsgegevens niet beter beveiligd te worden dan gebruikelijk

is om een toereikende kwaliteit van de informatievoorziening tot stand te brengen en in stand te houden. Als gevolg van de Wet bescherming persoonsgegevens worden voor deze risicoklasse geen extra eisen ten aanzien van de beveiliging gesteld dan welke al noodzakelijk zijn voor een zorgvuldige bedrijfsvoering. In deze studie zijn voor deze risicoklasse dan ook geen specifieke maatregelen opgenomen.

Risicoklasse I: Basis niveau
De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie. Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel -gast, vereniging - lid, organisatie - deelnemer. Opgemerkt wordt dat het lidmaatschap van een instelling op zich al informatie kan bevatten betreffende een persoon. Indien dit gegevens zijn die vallen onder de categorie bijzondere gegevens, bijvoorbeeld over politieke voorkeur, seksuele leven, kerkelijk genootschappen etc., dan dient de beveiliging van persoonsgegevens tenminste te worden ondergebracht in risicoklasse II.

Risicoklasse II: Verhoogd risico
De uitkomst van de analyse toont aan dat er extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. De te nemen (informatie)beveiligingsmaatregelen moeten voldoen aan hogere normen dan die gelden voor het basis niveau. In deze klasse passen bijvoorbeeld verwerkingen van persoonsgegevens die voldoen aan een van de hieronder gegeven beschrijvingen:

1. de verwerkingen van bijzondere persoonsgegevens zoals bedoeld in artikel
1. 16 WBP;
2. de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene;
3. de gegevens die bij handelsinformatiebureaus worden verwerkt ten behoeve van kredietinformatie of schuldsanering;
4. de gegevens die worden verwerkt hebben betrekking op de gehele of grotedelen van de bevolking (de impact van op zich onschuldige gegevens overeen groot aantal betrokkene);
5. alle verwerkingen van persoonsgegevens die met het bovenstaande vergelijkbaar zijn. Soms moet de verwerking van bijzondere gegevens vanwege een hoge gevoeligheidsgraad in het maatschappelijk verkeer, bijvoorbeeld wanneer het gegevens over levensbedreigende ziektes betreft, ondergebracht worden in risicoklasse III.

Risicoklasse III: Hoog risico
Bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens kan het resultaat van deze verwerking een dermate vergroot risico voor de betrokkene opleveren dat het gerechtvaardigd is deze verwerking van persoonsgegevens in risicoklasse III te plaatsen. De maatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen. De verwerking van persoonsgegevens die in deze klasse passen zijn onder andere de verwerkingen die betrekking hebben op opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van de betrokkene ernstig kunnen worden geschaad indien dit onzorgvuldig of onbevoegd geschiedt. Bijzondere verwerkingen van persoonsgegevens, bijvoorbeeld een DNA-databank, vallen in deze klasse. Daarnaast valt de verwerking van persoonsgegevens waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze klasse. Deze geheimhoudingsplicht kan zowel wettelijk of anderszins formeel zijn geregeld door de overheid of door een private organisatie zijn ingevoerd voor haar

medewerkers. In relatie tot de indeling van persoonsgegevens in risicoklassen, wordt ook in het kader van een bewuste omgang met die persoonsgegevens, gebruik gemaakt van markering. Markering is het aangeven van de risicoklasse die van toepassing is op de persoonsgegevens die op deze gegevensdrager zijn vastgelegd. De gegevensdrager wordt dus, indien technisch mogelijk, voorzien van een redelijkerwijs zichtbaar kenmerk dat aangeeft hoe de persoonsgegevens op die drager behandeld dienen te worden. Gegevensdragers zijn alle media waarin of waarop de persoonsgegevens kunnen worden vastgelegd, zoals papier, CD-ROM's, diskettes en tapes, schijven en intern geheugen. De functie van markering is dat de risicoklasse van de persoonsgegevens direct zichtbaar is. Hierop dienen de maatregelen voor het bewaren en gebruik van de gegevensdragers te worden afgestemd. Markering van persoonsgegevens tot en met risicoklasse II is optioneel. Markering van de persoonsgegevens behorende bij risicoklasse III is noodzakelijk.

Beheerregeling applicaties van Sociale Zaken en Werkgelegenheid Gemeente Haarlem

Burgemeester en wethouders van de gemeente Haarlem;

gelet op het bepaalde in artikel 13 van de Wet bescherming persoonsgegevens;

gezien het Informatiebeveiligingsplan gemeente Haarlem

B E S L U I T E N :

vast te stellen het volgende:

BEHEERREGELING VOOR DE APPLICATIES VAN SOCIALE ZAKEN EN WERKGELEGENHEID

HOOFDSTUK 1. ALGEMENE BEPALINGEN

Artikel 1. Begripsbepalingen

Deze regeling verstaat onder:

I.	**de wet:**	de Wet bescherming persoonsgegevens (Stb 2000, 302); SUWI (29 november 2001)
II.	**autorisatie:**	het binnen de toepassingsprogrammatuur toekennen van het niveau van gebruikersmogelijkheden aan een persoon of afdeling of het binnen de toepassingsprogrammatuur toekennen van het niveau van gegevensverstrekking aan derden.
III.	**de verantwoordelijke:**	het college van burgemeester en wethouders, welke de dagelijkse verantwoordelijkheid over de applicaties van Sociale Zaken en Werkgelegenheid en Werkgelegenheid heeft opgedragen aan de coördinator beleid van Sociale Zaken en Werkgelegenheid;
IV.	**de beheerder:**	de functionaris die namens de verantwoordelijke de zorg heeft voor de applicaties van Sociale Zaken en Werkgelegenheid;

V. **informatiebeheer:** het geheel van activiteiten gericht op beleidsvoorbereiding ter zake van de applicaties van Sociale Zaken en Werkgelegenheid en Werkgelegenheid, de ontwikkeling van kwaliteits-procedures, beveiligingsprocedures, verstrekkingsprocedures en privacyprocedures, alsmede de coördinatie bij de uitvoering van deze procedures;

VI. **gegevensbeheer:** het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening;

VII. **applicatiebeheer:** het geheel van activiteiten gericht op het onderhouden en ondersteunen van de applicaties van Sociale Zaken en Werkgelegenheid Zaken en Werkgelegenheid en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening;

VIII. **privacybeheer:** het geheel van activiteiten gericht op de bescherming van de persoonlijke levenssfeer van degene, waarover gegevens zijn opgenomen, bij het gegevens verzamelen, gegevens verwerken en de informatievoorziening;

IX. **gegevensverwerking:** het ontlenen van gegevens aan documenten en bestanden en deze op een voorgeschreven wijze middels de applicaties van Sociale Zaken en Werkgelegenheid opnemen in een gegevensbestand;

X. **GWS4all:** de software, die wordt gebruikt om de applicaties van Sociale Zaken en Werkgelegenheid in te richten en bij te houden;

XI. **procedure:** de voorgeschreven wijze waarop een activiteit moet worden uitgevoerd;

XII. **brondocumenten:** documenten waaraan gegevens worden ontleend, die in aanmerking komen voor opname in de applicaties van Sociale Zaken en Werkgelegenheid.

XIII. **uitwijkregeling:** regeling vastgesteld door de verantwoordelijke, hetgeen voorziet in mogelijkheden om kritische bedrijfsprocessen buiten het gemeentehuis voort te zetten, in geval de voorzieningen in het gemeentehuis niet bruikbaar zijn.

XIV. **reconstructiemaatregelen:** het geheel van activiteiten dat is gericht op het operationeel krijgen van een kritisch bedrijfsproces in een andere locatie dan het gemeentehuis.

XV. **back-up:** kopie van gegevensbestanden opgeslagen op een ander medium dan de originele gegevensbestanden.

Artikel 2. De beheerfuncties

1. De beheerder van de applicaties van de Sociale Zaken en Werkgelegenheid en in die hoedanigheid informatiebeheerder en privacybeheerder.
2. De beheerder wijst een functionaris aan die wordt belast met het gegevensbeheer en voorziet daarbij tevens in diens vervanging; de aanwijzing maakt als bijlage 1 onderdeel uit van deze regeling.
3. De beheerder wijst een functionaris aan die wordt belast met het applicatiebeheer en voorziet daarbij tevens in diens vervanging; de aanwijzing maakt als bijlage 1 onderdeel uit van deze regeling.
4. De beheerder wijst functionarissen aan die worden belast met de gegevensverwerking; de aanwijzingen maken als bijlage 1 onderdeel uit van deze regeling.
5. De medewerkers van het cluster I&A zijn aangewezen als functionarissen, die zijn belast met het systeembeheer.

Artikel 3. Reikwijdte van de beheerregeling

De in deze regeling opgenomen bepalingen gelden voor de gegevens, die op grond van of krachtens een wettelijke regeling in de applicaties van Sociale Zaken en Werkgelegenheid zijn opgenomen en die onder de werkingssfeer van de Wet Bescherming Persoonsgegevens vallen.

Hoofdstuk 2. HET INFORMATIEBEHEER

Artikel 4. Toezicht, bevoegdheden en verantwoordelijkheden

1. De informatiebeheerder ziet toe op de naleving van de in deze regeling opgenomen bepalingen alsmede op een juiste uitvoering van de bij of krachtens de wet opgelegde verplichtingen ten aanzien van inrichting en bijhouding, alsmede de beveiliging van de applicaties van Sociale Zaken en Werkgelegenheid.

2. De informatiebeheerder voorziet jaarlijks in een planning van de beheeractiviteiten.

3. De informatiebeheerder neemt namens de verantwoordelijke deel aan buitengemeentelijk overleg inzake onderwerpen die het beheer van de applicaties van Sociale Zaken en Werkgelegenheid aangaan of hij voorziet in zijn vertegenwoordiging.

4. De informatiebeheerder voorziet in de administratieve beheerprocedures, voor zover hier niet door of bij een wettelijk regeling is in voorzien.

5. De informatiebeheerder is verantwoordelijk voor een tijdige en juiste actualisering van deze Beheerregeling.

Artikel 5. Plichten

Door of namens de informatiebeheerder wordt het gemeentebestuur (de verantwoordelijke) advies verstrekt op de navolgende aspecten die voortvloeien uit de applicaties van Sociale Zaken en Werkgelegenheid, te weten:

- De informatievoorziening;

- De beveiliging;
- De privacy;
- De gegevenskwaliteit.

Hoofdstuk 3. HET GEGEVENSBEHEER

Artikel 6. Toezicht, bevoegdheden en verantwoordelijkheden

1. De gegevensbeheerder is, namens de informatiebeheerder, verantwoordelijk voor de juistheid, actualiteit en betrouwbaarheid van de gegevens die opgenomen zijn of worden in de applicaties van de afdeling Werk en Welzijn.

2. Vanuit de in het vorige lid bedoelde verantwoordelijkheid is de gegevensbeheerder bevoegd de gegevensverwerkers aanwijzingen te geven inzake de opname, bijhouding en wijziging van gegevens. Deze aanwijzingen mogen niet strijdig zijn met de door of bij een wettelijk regeling gestelde regels.

3. De gegevensbeheerder is verantwoordelijk voor een juiste archivering van brondocumenten: vanuit deze verantwoordelijkheid kan hij de gegevensverwerkers op dit punt aanwijzingen geven.

Artikel 7. Plichten

1. a. De gegevensbeheerder draagt zorg voor de uitvoering en controle van de mutaties, die in de applicaties van de afdeling Werk en Welzijn worden/zijn aangebracht.
   b. De gegevensbeheerder ziet er op toe dat de fouten en afwijkingen, die hierbij worden geconstateerd, worden afgehandeld.
   c. Van bijzondere gebeurtenissen voortvloeiend uit de plichten genoemd onder de leden 1a. en 1b houdt de gegevensbeheerder een logboek bij.

2. Van stagnatie bij de in het vorige lid bedoelde mutatie- en controlewerkzaamheden doet de gegevensbeheerder direct mededeling aan de informatiebeheerder.

Hoofdstuk 4. HET APPLICATIEBEHEER

Artikel 8 Toezicht, bevoegdheden en verantwoordelijkheden

1. De applicatiebeheerder behandelt verzoeken van medewerkers van de gemeente Haarlem tot rechtstreekse toegang tot de applicaties van Sociale Zaken en Werkgelegenheid en kent het autorisatieniveau van de raadpleging toe.

2. De applicatiebeheerder kent in overleg met de informatiebeheerder de autorisatieniveaus toe aan de gegevensverwerkers.

3. De applicatiebeheerder beoordeelt de gevolgen van de installatie van nieuwe en/of gewijzigde versie van GWS4all.

4. De applicatiebeheerder beslist inzake de installatie van nieuwe of gewijzigde versies van GWS4all. Hij ziet er op toe dat alle in de bijlage 1 genoemde functionarissen op de hoogte zijn gesteld van deze installatie en ziet er op toe dat de gevolgen van deze installatie bij deze functionarissen bekend zijn.

5. De applicatiebeheerder kan de informatiebeheerder, de gegevensbeheerder, de privacybeheerder, de systeembeheerder, de gegevensverwerker en andere medewerkers

van de gemeente Haarlem, die direct toegang hebben tot GWS4all aanwijzingen geven met betrekking tot het gebruik van deze systemen. Hij kan met betrekking tot het gebruik gedragsregels opstellen en interne opleidingen ontwikkelen.

6. De applicatiebeheerder is verantwoordelijk voor de vormgeving en inhoud van documenten die rechtstreeks aan de applicaties van Sociale Zaken en Werkgelegenheid worden ontleend.

7. De applicatiebeheerder is verantwoordelijk voor de afhandeling van verzoeken omtrent statistische gegevens voor zover deze niet tot een persoon zijn te herleiden.

8. De applicatiebeheerder beheert de bij de applicaties van Sociale Zaken en Werkgelegenheid behorende documentatie.

9. De applicatiebeheerder neemt namens de verantwoordelijke deel aan buitengemeentelijk overleg inzake onderwerpen die het beheer van de applicaties van Sociale Zaken en Werkgelegenheid Zaken aangaan of hij voorziet in zijn vertegenwoordiging.

Artikel 9. Plichten

1. De applicatiebeheerder houdt een verzameling bij van de autorisaties die overeenkomstig artikel 8, lid 1 en 2, zijn toegekend.

2. De applicatiebeheerder verstrekt voorlichting aan de gegevensverwerkers met betrekking tot de gevolgen van een nieuwe of gewijzigde versie van GWS4all.

3. De applicatiebeheerder verzorgt - na overleg met de systeembeheerder - de communicatie bij storingen in de hard- en/of software. De applicatiebeheerder stelt direct de informatiebeheerder van de storing op de hoogte.

4. De applicatiebeheerder verzorgt het testen en evalueren van nieuwe versies van GWS4all.

5. De applicatiebeheerder ziet er op toe dat alle inlog-codes, die noodzakelijk zijn voor de toegang tot GWS4all, Suwi-inkijk/DKD en daarmee tot de verschillende processen, correct worden opgeslagen.

6. De applicatiebeheerder verzamelt alle problemen en klachten, die bij het gebruik van GWS4all ontstaan, en tracht, door inschakeling van de systeembeheerder of de leverancier, voor een oplossing te zorgen.

Hoofdstuk 5. HET PRIVACYBEHEER

Artikel 10 Toezicht, bevoegdheden en verantwoordelijkheden

1. De privacybeheerder heeft het dagelijkse toezicht op de naleving van de privacyvoorschriften die voortvloeien uit de wet.

2. De privacybeheerder kan op grond van het in het vorige lid genoemde toezicht, de medewerkers van Sociale Zaken en Werkgelegenheid aanwijzingen geven.

3. De privacybeheerder heeft het algehele toezicht op de naleving van de beveiligingsvoorschriften die voortvloeien uit de wet.

4. De privacybeheerder heeft het toezicht op de be- en afhandeling van verzoeken om gegevensverstrekking en is betrokken bij de eventuele bezwaarschriften die daaruit voortvloeien.

5. De privacybeheerder kan - ongevraagd - advies uitbrengen over alle procedures en producten, waarbij de bescherming van de persoonlijke levenssfeer in het geding is.

6. De privacybeheerder kan voor de afhandeling van verzoekschriften om gegevensverstrekking als bedoeld in artikel 11 één of meerdere medewerkers van het taakveld Belastingen aanwijzen.

Artikel 11 Plichten

De privacybeheerder behandelt alle verzoekschriften die op basis van de wet worden ontvangen.

Hoofdstuk 6. HET SYSTEEMBEHEER

Artikel 12 Toezicht, bevoegdheden en verantwoordelijkheden

1. De systeembeheerder is verantwoordelijk voor het technisch onderhoud van en de ondersteuning bij het gebruik van GWS4all, Suwi-inkijk/DKD.

2. De systeembeheerder is bevoegd direct maatregelen te treffen als de continuïteit van GWS4all of de daarin opgeslagen informatie acuut in het geding is, mits achteraf rapportage plaatsvindt aan de informatiebeheerder.

3. De systeembeheerder is verantwoordelijk voor de fysieke beveiliging van GWS4all.

4. De systeembeheerder is verantwoordelijk voor een zo optimaal mogelijk gebruik van de toegangsbeveiligingen tot GWS4all.

5. De systeembeheerder is bevoegd aanwijzingen te geven met betrekking tot:
   - het beheer van GWS4all;
   - het beheer van de betreffende bestanden.

Artikel 13 Plichten

1. Van de gegevensbestanden opgenomen in GWS4all maakt de systeembeheerder dagelijks minimaal één back-up, welke dagelijks wordt ondergebracht in een daartoe uitgeruste brandveilige kluis.

2. Installatie van gewijzigde of nieuwe versies van GWS4all geschiedt niet eerder dan dat daartoe instemming is verkregen van de applicatiebeheerder. Na verkregen instemming geschiedt de installatie zo spoedig mogelijk. Van stagnaties bij het installatieproces stelt de systeembeheerder de informatiebeheerder direct op de hoogte.

3. In geval van storingen binnen GWS4all lost de systeembeheerder het probleem zo spoedig mogelijk op of schakelt hier voor een derde in.

4. De systeembeheerder zorgt voor de beschikbaarheid van GWS4all en Suwi-inkijk/DKD overeenkomstig hetgeen daarover in het Informatiebeveiliginggsplan is vastgelegd.

5. De systeembeheerder stelt de informatiebeheerder op de hoogte van personele wisselingen inzake de systeembeheerderfunctie of de vervanging hierin.

Hoofdstuk 7. DE GEGEVENSVERWERKING

Artikel 14 Toezicht, bevoegdheden en verantwoordelijkheden

1. De gegevensverwerker is verantwoordelijk voor het verzamelen van gegevens.

2. De gegevensverwerker is, voor zover daartoe door de applicatiebeheerder geautoriseerd, verantwoordelijk voor het verwerken van de gegevens overeenkomstig de daarvoor geldende procedures, alsmede volgens de daarop in de handleidingen van GWS4all beschreven toepassing.

3. De gegevensverwerker is verantwoordelijk voor de archivering van de brondocumenten op grond waarvan hij/zij de gegevens heeft verwerkt.

Artikel 15 Plichten

Nadat de gegevens zijn verzameld worden zij binnen de vereiste wettelijke termijn verwerkt.

Hoofdstuk 8. OVERIGE BEPALINGEN

Artikel 16 Slotbepaling

De verantwoordelijke beslist in alle gevallen waarin deze regeling niet voorziet.

Artikel 17 Werkingsgebied

De in deze regeling opgenomen bepalingen gelden voor:

- De gegevens, die op grond van of krachtens een wettelijke regeling in de applicaties van Sociale Zaken en Werkgelegenheid zijn opgenomen.
- De in de applicaties van Sociale Zaken en Werkgelegenheid opgenomen persoonsgegevens, die onder de werkingssfeer van de Wet Bescherming Persoonsgegevens (Stb. 2000, 302) vallen.

Artikel 18 Inwerkingtreding

Deze regeling treedt in werking de dag nadat zij is afgekondigd.

Artikel 19 Bekendmaking

Bekendmaking van deze beheerregeling geschiedt door publicatie van het besluit via BIS/website en via insite/intranet.

Artikel 20 Citeertitel

Deze regeling wordt aangehaald als "Beheerregeling applicaties van Sociale Zaken en Werkgelegenheid".

Haarlem, 30 juni 2010

Burgemeester en wethouders van Haarlem,

Burgemeester,	Secretaris,
de heer B.B. Schneiders	mevrouw S. Borgers

Toelichting op de beheerregeling voor de applicaties van de hoofdafdeling Sociale Zaken en Werkgelegenheid gemeente Haarlem

Door de Wet Bescherming Persoonsgegevens worden technische en organisatorische verplichtingen gesteld voor registraties, waarin persoonsgegevens zijn opgenomen. Als gevolg daarvan wordt bij deze een beheerregeling vastgesteld voor de applicaties van de Hoofdafdeling Sociale zaken en Werkgelegenheid in gebruik bij de Hoofdafdeling Sociale zaken en Werkgelegenheid van de gemeente Haarlem. Hierin wordt de dagelijkse beheerpraktijk geregeld en worden de verschillende taken, verantwoordelijkheden en bevoegdheden verbonden aan deze registraties vastgesteld.
De noodzaak tot het regelen hiervan vloeit ook voort uit het informatiebeveiligingsbeleid opgenomen in het Informatiebeveiligingsplan van de gemeente Haarlem.

De beheerregeling moet aan een aantal voorwaarden en moet in ieder geval voorzien in de invulling van de volgende activiteiten:

- Informatiebeheer;
- Gegevensbeheer;
- Applicatiebeheer;
- Privacybeheer;
- Systeembeheer;
- Gegevensverwerking.

De opzet van de SUWI beheerregeling en de daarin genoemde functies heeft als leidraad gediend voor deze beheerregeling voor de applicaties van Sociale Zaken en Werkgelegenheid.

Bijlage 1 Aanwijzing van beheerfunctionarissen

Op grond van artikel 2 van de Beheerregeling applicaties van de Hoofdafdeling Sociale zaken en Werkgelegenheid wijst de manager van de Hoofdafdeling Sociale Zaken en Werkgelegenheid in zijn functie van beheerder van de applicaties van de Hoofdafdeling Sociale zaken en Werkgelegenheid de navolgende beheerfunctionarissen aan:

Gegevensbeheer

Als gegevensbeheerder is aangewezen, W. Mevissen
Als functioneel applicatiebeheerder is aangewezen, J. Kint

Gegevensverwerking

Als gegevensverwerkers zijn aangewezen:
Alle medewerkers van de afdeling Sociale Zaken en Werkgelegenheid.

Haarlem, 30 juni 2010

Bijlage Functieverdeling

Binnen de gemeente Haarlem zijn binnen het kader van de informatiebeveiliging de volgende personen aangewezen:

Leden Werkgroep informatiebeveiliging Sociale Zaken en werkgelegenheid:

- de manager van de Hoofdafdeling Sociale Zaken en Werkgelegenheid; de heer R.J.A. van Noort
- de informatiemanager; de heer W. Mevissen
- De netwerkbeheerder; de heer T. Bleeker
- De medewerker Kwaliteitszorg; mevrouw A. van der Kraan
- de functioneel applicatiebeheerder; de heer J. Kint

Leden uitwijkteam:

- De gemeentesecretaris; mevrouw S. Borgers
- de manager van de Hoofdafdeling Sociale Zaken en Werkgelegenheid; de heer R.J.A. van Noort
- de functioneel applicatiebeheerder; de heer J. Kint
- De netwerkbeheerder; de heer T. Bleeker
- de beveiligingscoördinator; de heer

Gemeentesecretaris:

mevrouw S. Borgers

de beveiligingscoördinator:

mevrouw A.L. van der Kraan

De Interne uitwijkcoördinator:

de heer R.J.A. van Noort

de informatiemanager:

De heer B.S.Z. Shukrula

de functioneel applicatiebeheerder:

De heer E.F. de Jong

het hoofd van de afdeling Informatievoorziening:

De heer M.C. Baas

De Database beheerder:

De heer A. van den Brand en de heer R.G. Evers

de netwerkbeheerder:

De heer F. Bleeker

De Facilitair manager:

mevrouw H. Koopman