Basis beveiligingsrichtlijnen Sociale Zaken en Werkgelegenheid

Gemeente Haarlem

Versie	: 3.1
Status	: definitief
Proces verantwoordelijke	: de heer E.H.L. Dorscheidt
Datum	: 6 oktober 2010 laatste wijzigingen 13 maart 2014

Inhoudsopgave

INHOUDSOPGAVE 3

1. ALGEMEEN 4

1.1. INLEIDING 4
1.2. REGELING SUWI 4
1.3. WBP / BIJLAGEN I, II EN III 4
1.4. GOEDKEURING 5

2. VERSIEBEHEER 6

2.1. WERKGROEP INFORMATIEBEVEILIGING SOCIALE ZAKEN EN WERKGELEGENHEID 6
2.2. VERANTWOORDING 6
2.3. UITVOERING EN EVALUATIE 7

3. BEVEILIGING 8

3.1. WAAROM BEVEILIGEN? 8
3.2. WAT BEVEILIGEN? 8
3.3. HARDWARE ..... **FOUT! BLADWIJZER NIET GEDEFINIEERD.**
3.4. SOFTWARE 9
3.5. GEGEVENS 9
3.6. DATACOMMUNICATIE VERBINDINGEN 10
3.7. DOCUMENTATIE 11
3.8. HET GEBOUW 11
3.9. WERKPLEK 12
3.10. CLEAR DESK EN CLEAR SCREEN BELEID 12

4. INFORMATIEBEVEILIGINGSBELEID 13

4.1. BELEIDSDOELSTELLING 13
4.2. SECTORALE WET- EN REGELGEVING 13
4.3. INFORMATIEBEVEILIGING 14
4.4. BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL 15
4.5. RAAKVLAKKEN MET ANDER BELEID 16
4.6. TAKEN, VERANTWOORDELIJKHEDEN EN BEVOEGDHEDEN 17
4.7. PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN 18

5. BEVEILIGINGSINCIDENTEN 21

5.1. AANPAK INCIDENTEN EN ZWAKKE PLEKKEN 21
5.2. MOGELIJKE INCIDENTEN 21
5.3. INCIDENTMELDING 21
5.4. AFHANDELING 22
5.5. RAPPORTAGE 22
5.6. ZWAKKE PLEKKEN IN DE BEVEILIGING 22
5.7. DISCIPLINAIRE MAATREGELEN 23

6. NALEVING 24

6.1. NALEVING VAN WETTELIJKE VOORSCHRIFTEN 24

OVERZICHT PROCEDURES, RAPPORTAGE & BIJLAGE BASIS BEVEILIGINGSRICHTLIJNEN SUWI 25

BIJLAGE II RISICOKLASSE 25

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 / Bijlagen I, II en III

Uitgangspunt van de informatiebeveiliging voor de verwerking van de persoonsgegevens is de Wet Bescherming Persoonsgegevens. Bijlagen I, II en III van de Regeling SUWI schrijven 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,

Handtekening:

Gemeentesecretaris, de heer J. Scholten

Plaats en datum: Haarlem,

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
2.0	6 oktober	de heer M. van Schoonhoven	Definitief	Up-date	W. Mevissen A.L. Kraan
2.1	13 september 2012	de heer M. van Schoonhoven	Definitief	Up-date	A.L. Kraan R.J. Voorsteegh
3.1	2013-2014	Mevrouw A.l. van der Kraan	Definitief	Volledige revisie	A.L. Kraan R.J. Voorsteegh

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:

- Angelica vd Kraan, security officer SZW (Medew. kwaliteit & innovatie, SZW/PO)
- Bob Voorsteegh (Medew. kwaliteit & innovatie, SZW/PO)
- Albert Bakker (applicatiebeheer SZW/PO)

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 security officer SZW 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 '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. Binnen de gemeente Haarlem kan iedere medewerker gebruik maken van de voorzieningen op de locaties Raakspoort, Stadhuis en Brinkmanpassage. Bij volledige en langdurige uitval van de hardware op één locatie kunnen de werkzaamheden op een andere locatie worden uitgevoerd. De Raakspoort beschikt tevens over een generator waarbij een deel van de voorzieningen in gebruik kan blijven.

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.

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.

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 '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 Raakspoort aan de Zijlvest 39 te Haarlem is op een aantal manieren beveiligd. Dit is vastgelegd in het Gemeentelijk Informatiebeveiligingsbeleid 2014-2018. 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 de Raakspoort zijn inbraakwerende voorzieningen getroffen in de vorm van bewegingsmelders. Er is een elektronische toegangsbeveiliging voor de Raakspoort. Tijdens avondopenstellingen is er ook 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 de procedure uitwijk 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:

- 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. Clear desk en clear screen beleid

De Gemeente Haarlem stelt een "clear 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 mogen niet toegankelijk zijn voor onbevoegden wanneer zij onbeheerd achterblijven, medewerkers gebruiken hiervoor de 'lock-functie' op hun computer (bij geen gebruik worden de werkstation automatisch na 15 minuten vergrendeld).
- Vertrouwelijke en/of privacygevoelige informatie wordt na het afdrukken onmiddellijk van de printer verwijderd. We maken gebruik van follow-me-printing waardoor printopdrachten pas afgedrukt worden na autorisatie met een persoonlijke toegangspas op de printer.

4. Informatiebeveiligingsbeleid

4.1. 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.

4.2. 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.

4.2.1. 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 bijlagen I, II en III van de Regeling SUWI. In deze bijlagen 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 de bijlagen I van de Regeling SUWI.

4.2.2. 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.

4.2.3. 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.

4.3. Informatiebeveiliging

Informatiebeveiligingsbeleid is volgens de Code voor Informatiebeveiliging[4] 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

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

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 security officer SZW 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.

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.

4.4. Beveiligingseisen ten aanzien van personeel

4.4.1. 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 een aparte geheimhoudingsverklaring.

4.4.2. 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.
Handreiking en richtlijnen zijn opgenomen in het kwaliteitszorgsysteem van afdeling Sociale Zaken en Werkgelegenheid. In alle werkoverleggen wordt minimaal eens per jaar nadrukkelijk aandacht besteed aan de omgang met persoonsgegevens, zodat alle medewerkers alert blijven.

4.5. 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 clear desk policy.

4.6. 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 ´Functieverdeling SUWI´ de vervanging vastgelegd.

4.6.1. 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.

Om zorg te dragen voor een jaarlijkse evaluatie en bijstelling van onderhavig Basis beveiligingsrichtlijnen wordt de functie van security officer SZW in het leven geroepen. De security officer SZW 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.

4.6.2. 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 security officer SZW.
- Mogelijke ontwikkelingen die de bedrijfsinformatie bedreigen.
- Bespreking van en toezicht op beveiligingsincidenten zoals gerapporteerd door de security officer SZW.
- 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.

4.6.3. Verantwoordelijkheden van security officer SZW

Door het college van B&W is security officer SZW in de rol van beveiligingsbeheerder SUWI benoemd (verder genoemd security officer SZW). De security officer SZW is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Basis beveiligingsrichtlijnen SUWI. De security officer SZW rapporteert periodiek (minimaal eens per jaar) aan het college van B&W en het directieteam, zo nodig zonder tussenkomst van de diverse afdelingsmanagers.
Onder security officer SZW 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.

Security officer SZW 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 security officer SZW verstrekt daarnaast gevraagd en ongevraagd adviezen om te komen tot het gewenste beveiligingsniveau.

4.7. 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*

4.7.1. 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.

4.7.2. 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:

4.7.3. 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.

4.7.4. 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.

4.7.5. 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.

4.7.6. 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 100% van alle mutaties in persoonsgegevens herleidbaar moet zijn tot een individuele medewerker die hiervoor verantwoordelijk is en dat zulks geldt voor 100% van alle raadplegingen.

5. Beveiligingsincidenten

5.1. 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).

5.2. 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.

5.3. Incidentmelding

De ontdekker van het incident meldt het incident, conform procedure 'Incidentenbeheer SUWI', aan via FIX.
Incidenten inzake de applicaties SZW, waaronder Suwi-net worden conform procedure 'Incidentenbeheer SUWI', aan de security officer SZW of aan de eigen lijnmanager die het vervolgens meldt aan de betreffende security officer SZW.

5.4. Afhandeling

5.4.1. 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).

5.4.2. Afsluiting na incident

Wanneer volgens de security officer SZW 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 security officer SZW (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 security officer SZW. Vervolgens vindt in het overleg van de security officer SZW en de lijnmanager een evaluatie plaats van de gebeurtenis.

5.5. Rapportage

Alle beveiligingsincidenten worden schriftelijk door de security officer SZW 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 security officer SZW rapporteert , indien er zich beveiligingsincidenten hebben voorgedaan, 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).

5.6. Zwakke plekken in de beveiliging

Gebruikers dienen (mogelijke) zwakke plekken in de beveiliging (inzake de applicaties SZW, waaronder Suwi-net) te melden (via Fix) aan de security officer SZW of de eigen lijnmanager die het vervolgens meldt (via fix) aan de betreffende security officer SZW. De security officer SZW 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.

5.7. Disciplinaire maatregelen

5.7.1. 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.

6. Naleving

6.1. 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)*
- *Mens Centraal (SaaS applicatie welke een aanvulling op de eigen werkprocessen en een verbinding tussen de afdelingen en de partners van de gemeente, waarbij relevante informatie op een inzichtelijke manier verzameld en in beeld wordt gebracht, met als doel bij te dragen aan een integraal klantbeeld)*

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

6.1.1. 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.

6.1.2. Overwegingen ten aanzien van systeemaudits

Het ministerie SZW heeft in samenwerking met het BKWI en diverse instanties producten ontwikkeld waarmee vastgesteld kan worden hoe de sociale dienst persoonsgegevens verwerkt. Deze producten zijn actueel toegankelijk op de site van het BKWI.

- Binnen de gemeente zal jaarlijks een interne meting plaatsvinden inzake de beveiliging van persoonsgegevens. Deze meting zal verricht worden door de security officer SZW.

Bijlage I: Overzicht procedures, rapportages & bijlagen

Procedure

Procedure 1. Autorisaties applicaties SZW
Procedure 2. Communicatie over beveiliging Sociale Zaken
Procedure 3. Gegevensverwerking applicatie Sociale Zaken
Procedure 4. Incidentenbeheer Sociale Zaken
Procedure 5. Instellen en opvragen auditlog
Procedure 6. Uitwijk
Procedure 7. Terugmeldingen en Correctieverzoeken DKD

Rapportage

Rapportage 1. Controle autorisaties Sociale Zaken
Rapportage 2. Controle Terugmeldingen en Correctieverzoeken DKD
Rapportage 3. Evaluatie beveiligingsbeleid en plan
Rapportage 4. Test reconstructie Sociale Zaken
Rapportage 5. Controle gegevensverwerking Sociale Zaken

Bijlage

Bijlage 1. Risico-inventarisatie en evaluatie Informatiebeveiliging Sociale Zaken
Bijlage 2. Kenmerken applicaties Sociale Zaken
Bijlage 3. Verklarende woordenlijst
Bijlage 4. Functieverdeling Sociale Zaken
Bijlage 5. Bewerkersovereenkomst
Bijlage 6. Geheimhoudingsverklaring
Bijlage 7. Aanvraagformulier autorisatie applicaties SZW
Bijlage 8. Voorbeeld Autorisatiematrix SZW
Bijlage 9. Protocol: ‘Regels voor veilig gebruik persoonsgegevens SZW’

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 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.

De aard van de gegevens die worden uitgewisseld via SUWI-net maakt dat op basis van boven staande risicoklassen de verwerking van persoonsgegevens vallen onder de risicoklassen II en in sommige gevallen zelfs onder risicoklassen 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.