Veiligheidskit
GIDS VOOR DE TOEPASSING VAN DE MINIMUMNORMEN

1 Inleiding.

Het doel van deze gids is de veiligheidsconsulenten van de OCMW's:

- de minimale veiligheidsnormen die werden gecreëerd door de werkgroep veiligheid van de BCSS – KSZ, te helpen begrijpen;
- op een eenvoudige en concrete manier de minimale veiligheidsnormen te helpen toepassen;
- in geval van twijfel als referentie te dienen.

De POD MI zal deze gids aanvullen met algemene en doelgerichte informatie en de veiligheidspagina's op internet schrijven die zijn gewijd aan de problemen die de veiligheidsconsulenten stellen.
De veiligheidsconsulenten van de POD MI die op dinsdagen permanentie hebben, kunnen echter slechts in algemene termen op uw vragen antwoorden, want ze zijn niet op de hoogte van de specifieke situatie van elk OCMW. Ze kennen immers niet de indeling van de plaatsen, de informaticaomgeving of de programma's die de OCMW's gebruiken.
Ze zullen op deze gids steunen om u te adviseren tijdens hun contacten met u.

2 Beschrijving van het document.

Er werd geprobeerd om elke minimale veiligheidsnorm op een zo eenvoudig mogelijke manier uit te leggen. Deze minimale veiligheidsnormen komen voort uit de toepassing van de ‘’Richtlijnen’’ bettreffende veiligheid op het niveau van de instellingen die deel uitmaken van het netwerk dat door de KSZ wordt beheerd»[1].
Het is aanbevolen de Richtlijnen betreffende veiligheid op het niveau van de instellingen die deel uitmaken van het netwerk dat door de KSZ wordt beheerd, zo aandachtig mogelijk te lezen.
Dit document evenals de meeste teksten in deze handleiding die de veiligheid van het netwerk van de sociale zekerheid regelen, zijn beschikbaar op de website van de KSZ op het adres http://ksz-bcss.fgov.be.
De website van de POD MI beschikt eveneens over een FAQ (**F**requently **A**sked **Questions** – **V**aak **G**estelde **V**ragen).
De POD MI werd in deze taak bijgestaan door

- de veiligheidsdienst van de KSZ (security@bcss.fgov.be).
- de drie regionale federaties van de Unies van Steden en Gemeenten die ons hun kennis en ervaring ter beschikking hebben gesteld;
- documentatie van de UVCW en de VVSG;
- de erkende gespecialiseerde veiligheidsdienst (EGVD) van de SmalS-MvM ;
- de administratieve cel van de OCMW’S;
- de veiligheidsconsulenten van de VCCV (veiligheidsconsulenten coördinatievergadering);
- de groep V-ICT-OR
- bepaalde informatieveiligheidsconsulenten van het OCMW.

Deze deelnemers beschikken over kennis, ervaring en informatiebronnen die toegankelijk zijn voor alle OCMW’s die deel uitmaken van het netwerk van de KSZ.
Deze handleiding zal uiteraard worden herzien en verbeterd op basis van de evolutie van de minimumnormen en de verbeteringen die men na verloop van tijd ontdekt, evenals de nieuwe technieken.
Aan het eind van de gids vindt u de precieze adresgegevens van deze verschillende partners.

[1] http://www.bcss.fgov.be/documentation/nl/s%E9curit%E9/richtlijnen.PDF

3 Wat is een veiligheidsconsulent?

De veiligheidsconsulent is een persoon die zich binnen de instelling, binnen een vereniging van OCMW's of binnen een erkende gespecialiseerde veiligheidsdienst die onder een tariefafspraak met het OCMW valt, bezighoudt met het geheel van de veiligheidsmaatregelen toegepast op de gegevens van sociale aard. Het is dus zijn taak te waken over de veiligheid:

i. van de toegang tot de sociale gegevens (sociale software, boekhoudsoftware, dossiers met documenten die sociale gegevens bevatten, enz.);
ii. van het gebruik ervan;
iii. van de fysieke en computeropslag;
iv. van de gebruikers van deze gegevens;
v. van het herstel van deze gegevens;
vi. van het naleven van de wet op de bescherming van de persoonlijke levenssfeer (http://www.privacy.fgov.be/normatieve_teksten/cao_81_NL.pdf).

De volledige definitie van de veiligheidsconsulent is opgenomen in het K.B. van 1993 van de KSZ (http://www.bcss.fgov.be/nl/Legislation/19930812.htm).

Hij zal tevens:

- toezien op de organisatie van te nemen maatregelen om te voldoen aan de minimale veiligheidsvoorwaarden : het veiligheidsplan opstellen, de acties van het OCMW coördineren, de gespecialiseerde diensten contacteren (informaticabedrijven, veiligheidsdiensten, enz.), de gebruikers van de verbinding sensibiliseren op het gebied van veiligheid, enz.;
- het meest relevante veiligheidsbeleid voor het centrum toelichten aan de OCMW-Raad, binnen de normen die de KSZ heeft gedefinieerd;
- als tussenpersoon fungeren tussen de OCMW-Raad, de Secretaris, de verschillende diensten, de maatschappelijke werkers of administratieve gebruikers van de verbinding, de KSZ, de POD Maatschappelijke Integratie, de informaticabedrijven, enz.;
- controleren of de veiligheidsregels worden nageleefd.

3.1 Wie kan veiligheidsconsulent worden?

Hoewel de rol van veiligheidsconsulent enkele technische aspecten inhoudt, bestaat deze in de eerste plaats uit coördinatie en communicatie. Daartoe zijn didactische vaardigheden om de collega's te sensibiliseren op het gebied van veiligheidsnormen een niet te verwaarlozen troef.
Daarom is het niet absoluut noodzakelijk deze taak toe te vertrouwen aan een technische expert, maar eerder aan een persoon die beschikt over relationele vaardigheden en een minimum aan interesse in technische en informatica-aspecten.

Opmerking : het is niet aanbevolen de informaticaverantwoordelijke te benoemen als veiligheidsconsulent.

De veiligheidsconsulent moet niet in het bezit zijn van een specifiek diploma of beroepsopleiding. Er kan echter een opleiding worden gevolgd. Voor het ogenblik organiseert de POD MI infosessies, terwijl de SmalS-MvM een veeleer technische opleiding geeft.

Het OCMW kan één of meer adjuncten aanduiden om de veiligheidsconsulent bij te staan bij de uitvoering van zijn taken.

3.2 Hoe benoemt u een veiligheidsconsulent?

De benoeming van de veiligheidsconsulent moet het onderwerp uitmaken van een beslissing van de OCMW-raad. Deze beslissing met vermelding van de identiteit en de professionele gegevens van de veiligheidsconsulent en, in voorkomend geval, zijn adjuncten moet aan de Informatieveiligheidsdienst van de POD Maatschappelijke Integratie worden meegedeeld:
POD Maatschappelijke Integratie G. Kempgens (veiligheidsconsulent)
Anspachlaan 1 1000 Brussel Tel.: 02/508.86.56 Fax:
De OCMW-raad moet tevens het aantal uren bepalen dat aan de veiligheidsconsulent (en zijn adjuncten) wordt toegekend om zijn opdracht te vervullen. Er bestaat geen regel om het aantal uren te bepalen dat nodig is voor de veiligheidsconsulent: dat is grotendeels afhankelijk van de situatie waarin het OCMW zich bevindt. Uiteraard moet er, eens de veiligheidsmaatregelen zijn geïnstalleerd, enkel nog opvolging gebeuren. Voor deze opvolging is vanzelfsprekend minder tijd nodig.

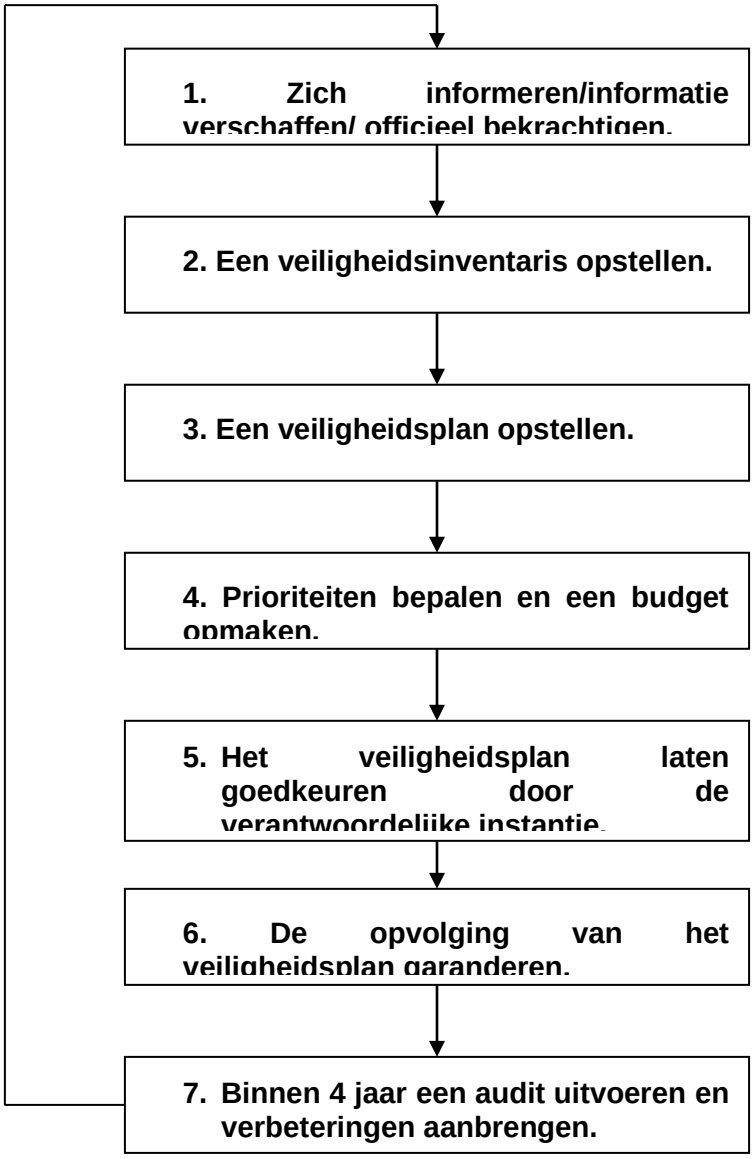
3.3 Wat doet een veiligheidsconsulent ?

De belangrijkste taak van de veiligheidsconsulent is, via een veiligheidsplan, ervoor te zorgen dat het OCMW voldoet aan de minimale veiligheidsnormen die de KSZ eist. Daarnaast zijn er de praktische aspecten die in dit deel worden uiteengezet. Het succes van het veiligheidsbeleid berust eveneens op het coördinerende werk van de consulent: relevante informatie verschaffen aan de OCMW-raad, de gebruikers sensibiliseren op het gebied van de veiligheidsnormen, als contactpersoon optreden voor de leveranciers van het OCMW, enz.
Onder de normen die de KSZ heeft gedefinieerd, werden als vervolg op deze gids vier soorten van maatregelen ontwikkeld:

1. maatregelen die duidelijke regels vastleggen op het gebied van communicatie en overleg tussen de veiligheidsconsulent en de verschillende onderdelen van het OCMW;
2. maatregelen die een fysieke beveiliging garanderen van de gegevens tegen materiële degradatie (diefstal, brand- of overstromingsschade, elektriciteitspanne, enz.);
3. maatregelen die een logische beveiliging van de gegevens garanderen tegen informaticagebonden risico's (computervirussen, verlies van gegevens, identificatie van de gebruikers, enz.);
4. maatregelen die bijdragen tot het onderhoud en de aanpassing van de veiligheidsregels tegenover de technische ontwikkeling (updaten van de programma's of van informaticamateriaal) of tegenover evenementen die zich kunnen voordoen.

Veiligheidskit
GIDS VOOR DE TOEPASSING VAN DE MINIMUMNORMEN

Om uw veiligheidsproces te realiseren, stellen wij u een voorbeeld van een werkplan voor dat uit verschillende stappen bestaat. Het ziet eruit als volgt:



De richtlijnen en minimumnormen lezen. Het personeel inlichten over uw rol.

Een fysieke (meubelen, materiaal, lokalen) en logische (programma's, toepassingen, licenties) inventaris opmaken.

De lijst opstellen van te realiseren taken (zie voorbeeld van veiligheidsplan op de website van de SPP IS).

4 en 5
Uw werk per kwartaal plannen, een budget voor 3 jaar opmaken en het laten goedkeuren door de OCMW-raad.

Bepalen hoe vaak er zal worden geëvalueerd en de veiligheidssystemen, registraties en controle-systemen opvolgen.

4 Te ondernemen stappen voor het naleven van de minimale veiligheidsnormen.

4.1 Minimale veiligheidsnormen voortkomend uit het Koninklijk Besluit van 12/08/1993.

Norm 4.1.1 : elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over een veiligheidsconsulent beschikken of deze taak toevertrouwen aan een erkende gespecialiseerde informatieveiligheidsdienst.

De persoon belast met het dagelijks bestuur van het OCMW kiest voor één van de voorgestelde mogelijkheden, waarbij rekening wordt gehouden met:

- artikels 24 en 25 van de wet van 15/01/1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid;
- het KB van 12/8/1993 betreffende de organisatie van de informatieveiligheid in de sociale-zekerheidsinstellingen;
- advies nr. 99/09 van 9 november 1999 van het Sectoraal Comité van de Sociale Zekerheid betreffende de verschillende vragen gesteld door de FOD Sociale Zekerheid met betrekking tot de veiligheidsconsulenten van de OCMW's;
- de specifieke behoeften van zijn/haar organisatie.

1.1 Mogelijkheid 1 (beschikken over een veiligheidsconsulent).
Intern een veiligheidsconsulent benoemen: er wordt u een bijkomend selectiemiddel ter beschikking gesteld, getiteld "Gedragscode voor de veiligheidsconsulenten"[2].

1.2 Mogelijkheid 2 : (de taak toevertrouwen aan een erkende gespecialiseerde informatieveiligheidsdienst)
Het moet hier gaan om een klein OCMW.
Het OCMW legt de vraag vooraf ter goedkeuring voor aan het Sectoraal Comité van de Sociale Zekerheid.
Om het Sectoraal Comité in staat te stellen de omvang van het betrokken OCMW te beoordelen, zal de aanvraag het aantal personeelsleden, het aantal informatici en het aantal gebruikers van het OCMW en het aantal dossiers in beheer vermelden.
Het OCMW neemt contact op met de erkende gespecialiseerde informatieveiligheidsdienst om de voorwaarden te bepalen en/of de samenwerking te bevestigen.

1.3 Mogelijkheid 3: een veiligheidsconsulent aanstellen die ook ter beschikking gesteld wordt aan een of meerdere OCMW's (dit kan via een convenant van terbeschikkingstelling).

1.4 Mogelijkheid 4: een vereniging hoofdstuk XII creëren die het mogelijk maakt een veiligheidsconsulent te benoemen.
Een vereniging hoofdstuk XII kan een veiligheidsconsulent benoemen die zich uitsluitend zal bezighouden met de veiligheid binnen verschillende OCMW's. Deze oplossing kan praktisch zijn, maar men mag tevens niet te veel OCMW's toevertrouwen aan één consulent opdat zijn workbelasting niet te hoog zou zijn.

1.5 Mogelijkheid 5: een beroep doen op een intercommunale of een openbare instelling die een veiligheidsconsulent tot uw beschikking stelt door middel van een conventie die de beschikbaarstelling dekt.
Dit biedt een OCMW de mogelijkheid om een veiligheidsconsulent te laten benoemen die is tewerkgesteld door een openbare instelling (intercommunale, interregionale), op voorwaarde

[2] http://www.bcss.fgov.be/documentation/nl/s%E9curit%E9/ethgedrag.PDF

dat deze instelling door de KSZ is erkend. Opmerking: er kan tevens een persoon van de gemeente worden aangesteld als veiligheidsconsulent. In dat geval zal er tussen het OCMW en de gemeente een conventie worden getekend die, onder andere, specifieert dat de veiligheidsconsulent tijdens zijn prestaties uitsluitend verantwoording aflegt aan de persoon die is belast met het dagelijks bestuur van het OCMW.

Ten slotte kan het ook nog goed zijn te preciseren dat de veiligheidsconsulenten zich technisch kunnen laten adviseren door een privé-leverancier. Deze leverancier kan echter niet worden aangesteld als veiligheidsconsulent.

Meer details vindt u op de website van de KSZ op het volgende adres:
http://ksz-bcss.fgov.be/documentation/nl/documentation/S%E9curit%E9/V2002.071.CSICPAS.nl1.pdf

Norm 4.1.2. : elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet de identiteit van zijn veiligheidsconsulent en zijn eventuele adjuncten meedelen aan de POD Maatschappelijke Integratie.

De persoon belast met het dagelijks bestuur van het OCMW deelt de beslissing van de OCMW-raad via een gewoon schrijven mee aan de POD Maatschappelijke Integratie, alsmede de identiteit van zijn veiligheidsconsulent of van de erkende gespecialiseerde veiligheidsdienst van zijn keuze.

De benoeming van een veiligheidsconsulent moet het voorwerp uitmaken van een beslissing van de OCMW-raad.

OPMERKINGEN : de aansluiting van het OCMW op het netwerk dat wordt beheerd door de KSZ, is onderworpen aan het meedelen aan de POD Maatschappelijke Integratie van de identiteit van zijn informatieveiligheidsconsulent of van de samenwerking met een erkende gespecialiseerde informatieveiligheidsdienst.
Om de missie van de consulent binnen een OCMW te bevorderen, is het aanbevolen dat de persoon die is belast met het dagelijks bestuur, deze functie officieel bekrachtigt en aan het personeel uitlegt wat de doelstellingen, voordelen en verplichtingen van het OCMW zijn om het netwerk van de sociale zekerheid te kunnen gebruiken.

Het kan nuttig zijn enkele basistaken van de veiligheidsconsulent te herhalen, die onder andere:

- aan de verantwoordelijke voor het dagelijks bestuur van het OCMW een voorstel van een veiligheidsplan moet voorleggen voor een periode van drie jaar, waarin de benodigde middelen voor de uitvoering ervan vermeld staan;
- het opstellen van een rampenplan eigen aan zijn OCMW moet coördineren;
- moet toezien op de naleving van de minimale veiligheidsnormen binnen zijn OCMW;
- de bevoorrechte contactpersoon moet zijn van de veiligheidsdiensten van de POD MI en de KSZ;
- moet waken over de naleving van de procedures op het gebied van toegang tot het netwerk van de gebruikers.

Norm 4.1.3. : wanneer binnen het OCMW de beroepskaart voor een geneeskundige verzorging (de SAM-kaart) wordt gebruikt, dan moet de veiligheidsconsulent binnen zijn OCMW waken over het veilige gebruik van deze kaart zoals vastgelegd in artikels 42 tot en met 50 van het Koninklijk Besluit van 22 februari 1998.

De SAM-kaarten zijn elektronische chips vergelijkbaar met degenen geïntegreerd in de SIS-kaart. Deze SAM-kaarten moeten gebruikt worden om de gegevens te kunnen inlezen die in de chip van de SIS-kaart staan ingeschreven. Bepaalde OCMW'S gebruiken ze voor hun behoeften. In dit geval moet de veiligheidsconsulent een inventaris bijhouden:

- nummers van de SAM-kaarten;
- namen van de gebruikers;
- nummers van de SAM-kaartlezers;

en natuurlijk deze inventarissen geactualiseerd houden. De SAM-kaart wordt door INAMI uitgereikt maar de Heer J. Mertens van SmalS-MvM (02.509.58.85) kan, op aanvraag, u de bestaande procedure uitreiken om de SAM-kaarten te verkrijgen en te weten wat u in geval van verlies of vlucht moet doen.
Een andere informatie betreffende de SAM- en de SIS-kaarten is beschikbaar op het volgende adres: *http://www.ksz.fgov.be/nl/documentation/document_3.htm.*

Veiligheidskit
GIDS VOOR DE TOEPASSING VAN DE MINIMUMNORMEN

Norm 4.1.4. : elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank van de Sociale Zekerheid, moet aan de Kruispuntbank het aantal uren meedelen dat het officieel aan de veiligheidsconsulent en aan zijn eventuele adjuncten heeft toegekend voor de uitvoering van hun taken.

Deze informatie wordt elk jaar opgevraagd door de POD MI in een vragenlijst gericht aan de veiligheidsconsulenten van de OCMW's (Vragenlijst voor het uitvoeren van de minimale veiligheidsnormen). Deze informatie wordt vervolgens doorgestuurd naar de KSZ die ze meedeelt aan het Sectoraal Comité voor de Sociale Zekerheid.
Deze jaarlijkse vragenlijst wordt over het algemeen ingevuld door de veiligheidsconsulent van het OCMW. Ze moet vervolgens worden ondertekend door de persoon dis is belast met het dagelijks bestuur van het OCMW en doorgestuurd naar de bevoegde dienst van de POD Maatschappelijke Integratie.

Het aantal uren dat de veiligheidsconsulent nodig heeft om zijn opdracht uit te voeren, moet niet worden gebaseerd op een verdeling van zijn tijd op basis van de andere rol(len) die hij binnen het OCMW heeft, maar eerder op criteria zoals de tijd nodig om:

- binnen de termijnen, elk punt van het oorspronkelijke veiligheidsplan uit te voeren;
- deel te nemen aan interne vergaderingen over veiligheidsaspecten;
- een veiligheidsbeleid op te stellen en aan te houden dat voor zijn OCMW de toegang regelt tot het netwerk dat door de KSZ wordt beheerd;
- zijn collega's te sensibiliseren op het vlak van veiligheid;
- zijn rol te verzekeren als tussenpersoon voor het verlenen van toegangsrechten met de POD MI of de administratieve cel van de OCMW's;
- deel te nemen aan werkvergaderingen georganiseerd door de POD MI;
- de rapporten op te stellen voor de persoon die is belast met het dagelijks bestuur van zijn OCMW;
- de toekomst voor te bereiden door opleidingen te volgen of zich in te lichten over de technologische evolutie die zich binnen het netwerk ontwikkelt of wordt gebruikt binnen zijn organisatie;
- de vragenlijst over de minimumnormen te beantwoorden;
- het nieuwe veiligheidsplan voor te bereiden.

Kijk ook op het veiligheidsplan dat op de website van de POD MI staat voor concrete tijdsindicaties per taak.

Norm 4.1.5. : elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over een formeel informatieveiligheidsbeleid beschikken dat voortdurend wordt geactualiseerd.

Een veiligheidsbeleid is een document dat het belang preciseert dat het OCMW hecht aan zijn bezittingen (meubilair, informatica, kennis, enz.), en de middelen en prioriteiten die hieraan worden toegewezen.

Het informatieveiligheidsbeleid van elk OCMW moet beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

Het veiligheidsbeleid is een document gecreerd door een veiligheidsconsulent en goedgekeurd door de sociale raad / het vast bureau. Het document toont aan wat de risiko's zijn die het OCMW in acht wil nemen.

Voorbeeld.
Het OCMW verondersteld dat zijn goede werking afhangt van de kennis van het personeel op het vlak van sociale hulp, van de leefloon en het geheel van diensten die overeenstemmen met de mensen die het nodig hebben. Het OCMW moet zijn middelen met aandacht beheren en de gepaste maatregelen nemen tegen schade.
De bedreigingen die het personeel, de bezittingen en zijn bezoekers schade kunnen berokkenen, bevatten agressie naar werknemers toe, de ongeautoriseerde toegang, diefstal, fraude, vandalisme, brand, natuurrampen, technische storingen en toevallige schadegevallen.
De bedreigingen zoals "cyberattack"[3] en de acties met slechte bedoelingen via internet komen veel voor en kunnen veel schade aan de electronische diensten en aan de essentiele infrastructuur berokkenen.
Het OCMW veiligheidsbeleid schrijft de toepassing van beschermingsmaatregelen voor om het risiconiveau te verminderen. Het veiligheidsbeleid is voorzien om de werknemers te beschermen, de vertrouwelijkheid te vrijwaren, de beschikbaarheid, de integriteit en de waarde van al de bezittingen van het OCMW waar te nemen en de permanente werking van de diensten te kunnen verzekeren. Daar het OCMW persoonlijke gegevens langs zijn informaticasystemen laat verwerken in het kader van zijn dagelijkse activiteiten onderstreept het beleid de belangrijkheid van de electronische handelingen te controleren.

Het OCMW zal dus een veiligheidsbeleid opstellen betreffende de risiko's die ze zelf als het grootst beschouwt. Worden in acht genomen:

- personeel;
- de documentatie;
- de logische en fysieke toegangen;
- enz.

Het is belangrijk te herineren dat een veiligheidsbeleid min of meer strict zal zijn in functie van de mogelijke risico's: misdadigheid, directe nabijzijn van een rivier, oud houten gebouw, enz.
Om de OCMW's en de sociale zekerheidsinstellingen te helpen en hen in staat te stellen het doel gemakkelijker te bereiken, heeft de werkgroep "Informatieveiligheid" van het Algemeen Coördinatiecomité van de Kruispuntbank van de Sociale Zekerheid een ISMS (**I**nformation **S**ecurity **M**anagement **S**ystem) ontwikkeld. Dit basisdocument dat gemeenschappelijk is voor alle instellingen die zijn aangesloten op het netwerk, wordt tot uw beschikking gesteld op de website van de KSZ; Het moet echter worden aangepast aan de specifieke behoeften van elk OCMW.

[3] Cyberattack is een electronische aanval van een gespecialiseerde persoon met een goede informaticakennis en die zich toegang wil verschaffen tot de documenten om ze te raadplegen, te vernietigen of te veranderen.

Veiligheidskit
GIDS VOOR DE TOEPASSING VAN DE MINIMUMNORMEN

1. informatie-veiligheidsbeleid Definitie van de doelstellingen	Een veiligheidsbeleid creëren door aan te geven dat men in functie van de risico's wil beschermen. *Voorbeeld: is het OCMW dichtbij een rivier? Het doel: anticiperen op de mogelijke schade van een overstroming.* Dit beleid herzien in functie van de risico's, de veiligheid organiseren en de vereiste budgetten vrijmaken.
2. Organisatie van de veiligheid	De veiligheid organiseren in functie van de doelstellingen *Voorbeeld: een waterdetector plaatsen en er voor zorgen dat een persoon wordt verwittigd.*
3. Inventaris van de hulpbronnen analyse van de risico's.	In functie van wat het OCMW wil beschermen (bepaald in het veiligheidsbeleid), een inventaris opmaken van wat noodzakelijk is om het risico te verminderen of om een mogelijkheid tot vervangen te hebben. Het risico moet geëvalueerd worden. V*oorbeeld: wat is het overstromingsrisico? Overstromingen in 1996 en in 2001, dus risico dreigt. Als het water tot 50 cm stijgt zoals in 1996, hoe kan men de server of PC beschermen? Zoniet, hoe de gegevens terugkrijgen?*
4. Selectie en toepassing van de controles	Een oplossing kiezen evenredig met het risico. Als de schade gemakkelijk te herstellen is, niet roekeloos investeren. V*oorbeeld: controleren of laten controleren of het systeem werkt. Een detector van water zal het mogelijk maken om op tijd te reageren en om het materiaal te redden. De detector onderhouden.*
5. Continuïteitsplanning	Het continuïteitsplan is het document dat het OCMW moet toelaten om opnieuw te beginnen werken in geval van een gedeeltelijk of een totaal probleem.
6. Opleiding	Het kan voorzien zijn om een opleiding te organiseren of om een opleiding te laten volgen om gewoon te worden in geval van problemen te reageren. *voorbeeld: oefening van evacuatie van de lokalen, herinstallatie van de backup, controleren dat de bescherming van de gegevens echt werd uitgevoerd.*
7. Documentatie	De veiligheidsdoelstellingen documenteren die in het veiligheidsbeleid zijn opgenomen *Voorbeeld: detail van de acties die in geval van overstroming moeten ondernomen worden.*
8. Controle en audit	De controles worden door de consulent verricht, de audit wordt door een andere persoon uitgevoerd. De audit heeft ten doel de doeltreffendheid of de inefficiëntie van de veiligheid aan te tonen. De audit moet het mogelijk maken om de veiligheid te verbeteren. *Voorbeeld: heeft de te volgen procedure in geval van overstroming alles voorzien? Wat doet men als de verantwoordelijke persoon afwezig is?*

De teksten met betrekking tot de informatie in dit hoofdstuk zijn beschikbaar op de website van de KSZ op: http://ksz-bcss.fgov.be/nl/securite/securite_home.htm

De eventuele verbeteringen aan te brengen aan het veiligheidsbeleid van het OCMW kunnen, mits toelating van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Veiligheidskit
GIDS VOOR DE TOEPASSING VAN DE MINIMUMNORMEN

Norm 4.1.6 : elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank; moet in het bezit zijn van een veiligheidsplan dat door de verantwoordelijke instantie van het betrokken OCMW werd goedgekeurd.

Het jaarlijkse veiligheidsplan beschrijft de prioriteiten van de veiligheidsconsulent in de loop van de drie komende jaren. Als het veiligheidsplan dat is opgesteld in 2005, acties voor 2006 bevat, dan zal het naar alle waarschijnlijkheid veel gedetailleerder zijn dan voor 2007en 2008 aangezien de prioriteiten wel bekend zullen zijn en de informatica en wetgeving mettertijd geëvolueerd zullen zijn.

Het veiligheidsplan is de formele en schriftelijke versie van het veiligheidsbeleid van het OCMW. Het is het traject dat de veiligheidsconsulent moet volgen om te voldoen aan de minimale veiligheidsnormen van de KSZ. Het gaat tevens om een bewijsstuk dat rekening houdt met het actieve veiligheidsbeleid van het OCMW.
Het veiligheidsplan dat door de veiligheidsconsulent wordt voorbereid, moet worden goedgekeurd door de OCMW-raad die regelmatig (minstens één keer per kwartaal) op de hoogte moet worden gehouden van de vooruitgang in de toepassing ervan en de wijzigingen waarvan het plan het onderwerp uitmaakt, moet goedkeuren.
Bovendien zal de OCMW-raad de mogelijkheid analyseren om de nodige middelen vrij te maken voor de uitvoering van het veiligheidsplan. Als de uitgaven te voorzien zijn, dan zullen ze het voorwerp uitmaken van een specifieke budgetpost.

Op basis van een overzicht (analyse) van de bestaande veiligheidsmaatregelen in het OCMW, in de verschillende domeinen van de informatieveiligheid (organisatorisch, fysieke beveiliging, logische beveiliging van de toegang tot de gegevens, ontwikkeling en onderhoud van de toepassingen, bescherming van het netwerk, continuïteitsplan,...) en de nog te nemen maatregelen om de situatie te optimaliseren en zo te voldoen aan de minimale veiligheidsnormen, kan de informatieveiligheidsconsulent van het OCMW het veiligheidsplan van zijn OCMW opstellen (inventaris van de te ondernemen stappen en eventueel te maken kosten).
Het veiligheidsplan dat onder andere titels kan worden voorgesteld zoals administratieplan, moet rekening houden met de specifieke situatie van het OCMW en de te beveiligen werkingsmiddelen. In elk geval zal de veiligheidsconsulent de te ondernemen stappen en de kosten die eruit voortvloeien moeten spreiden in de tijd.
Een voorbeeld van een veiligheidsplan is beschikbaar op de website van de POD MI: http://mi-is.be.

Een veiligheidsplan kan slagen op voorwaarde dat:
- de te vervullen taken worden gedefinieerd;
- de verschillende actoren bij de uitvoering ervan worden gedefinieerd;
- de opeenvolging en de prioriteit van de verschillende taken worden gedefinieerd;
- de nodige menselijke, materiële en financiële middelen worden ingezet voor de realisatie ervan.

Net als voor alle veiligheidsmaatregelen moeten de maatregelen die zijn voorgesteld in het plan, beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

Voorbeeld

Veiligheidsnorm	Situatie	Genomen maatregelen	Te nemen maatregelen	Deadline	Budget
Norm 4.3.3. Alternatieve stroomvoorziening	Het OCMW beschikt over een server die alle gegevens en naar de KSZ gestuurde berichten centraliseert. Het coderen van de dossiers die naar de KSZ worden doorgestuurd, gebeurt rechtstreeks op de server. De server beschikt voor het ogenblik niet over een alternatieve stroomvoorziening.	Geen	Aankoop van een noodvoeding om op de server aan te sluiten.	1/1/2006	250 €

Norm 4.1.7. Elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over de nodige werkkredieten beschikken die door de verantwoordelijke instantie van het betrokken OCMW werden goedgekeurd, en die in een afzonderlijk gedefinieerd veiligheidsbudget zijn opgenomen, teneinde te kunnen voorzien in de uitvoering van zijn veiligheidsplan.

De toepassing van de veiligheidsmaatregelen waarin is voorzien in het veiligheidsplan, kan soms grotere of kleinere kosten met zich meebrengen afhankelijk van hun omvang. Om de veiligheidsconsulent in staat te stellen deze kosten aan te gaan, kunnen ze, mits toestemming van de persoon die is belast met het dagelijks bestuur, worden opgenomen in het werkingsbudget van het OCMW. Dankzij een dergelijke organisatie beschikt de veiligheidsconsulent over het nodige budget voor de realisatie van de veiligheidsmaatregelen in zijn veiligheidsplan.

Deze kredieten moeten in verband worden gebracht met het veiligheidsplan. Op basis van de beschikbaar gestelde financiële middelen zal men keuzes moeten maken en prioriteiten stellen. De persoon die is belast met het dagelijks bestuur van het OCMW, moet op dit vlak de rol van scheidsrechter kunnen waarnemen en de prioriteiten bepalen onder de taken die de veiligheidsconsulent heeft geformuleerd.

Net als voor alle veiligheidsmaatregelen moeten de in het plan voorgestelde maatregelen beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

Om u concrete hulp te bieden zonder echter de boekhoudkundige organisatie van uw OCMW precies te kennen, stellen wij u voor de inschrijving van het budget “Veiligheid” in het globale budget van uw OCMW te optimaliseren in overleg met de persoon die is belast met het dagelijks bestuur van uw OCMW.
Bijvoorbeeld: de geplande onkosten voor de realisatie van de veiligheidsmaatregelen die in het veiligheidsplan zijn opgenomen, voor het referentiejaar, kunnen het onderwerp uitmaken van een afzonderlijk budget of van één of meer afzonderlijke budgetartikels met als titel bijvoorbeeld:

- « Werkingskosten voor de beveiliging van de informatieverwerking » ;
- en/of
- « Investeringskosten voor de beveiliging van de informatieverwerking ».

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

4.2 Minimale veiligheidsnormen die zijn gedefinieerd door de werkgroep "Informatieveiligheid".

4.2.1 Veiligheidsorganisatie.

Norm 4.2.1.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over procedures beschikken met het oog op de communicatie van informatie aan de veiligheidsconsulent, zodanig dat hij over de gegevens beschikt voor de uitvoering van de hem toegewezen veiligheidsopdracht.

De taken van de veiligheidsconsulent bestaan grotendeels uit de coördinatie van de verschillende onderdelen van het OCMW: mandatarissen, secretaris, sociale en administratieve diensten, technische diensten, enz. De KSZ vraagt dat de formele maatregelen voor communicatie en overleg worden vastgelegd opdat de veiligheidsconsulent zijn plaats vindt in de organisatie van het OCMW.

Om zijn missie te vervullen heeft de veiligheidsconsulent informatie nodig over de praktische organisatie van het OCMW. Deze behoefte is des te groter als de veiligheidsconsulent nog maar pas is opgenomen in het OCMW of niet permanent op het OCMW aanwezig is: dit is bijvoorbeeld het geval wanneer het OCMW ervoor heeft gekozen een consulent te benoemen samen met andere OCMW's, een gemeentelijke preventieambtenaar te benoemen of een erkende gespecialiseerde veiligheidsdienst in te schakelen.
Er moet dus in formele procedures worden voorzien die het mogelijk maken de consulent op de hoogte te houden van elementen die van nabij of van ver met veiligheidskwesties te maken hebben. Bijvoorbeeld:

- veiligheidsproblemen: wanneer, waar en hoe veiligheidsproblemen zich hebben voorgedaan (degradatie van het materiaal, onmogelijkheid om de verbinding met de KSZ te maken, aanval van een computervirus, enz.);
- organisatie van de OCMW-diensten: hoe de diensten georganiseerd zijn, wie wat doet, wie belast is met het ingeven van de beslissingen, welke maatschappelijke werker de gegevens op het netwerk van de sociale zekerheid moet kunnen raadplegen, welke personeelsveranderingen zijn opgetreden (aanwerving, vertrek, verandering van post, enz.).

Concreet en bij wijze van voorbeeld vermelden we het instellen van mondelinge of schriftelijke procedures om te garanderen dat de veiligheidsconsulent kan deelnemen aan de vergaderingen van de verschillende diensten (informaticawerken, preventie en bescherming op het werk,...) en/of de nodige verslagen van vergaderingen ontvangen voor de uitvoering van zijn taak.

Norm 4.2.1.2. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over procedures beschikken met als doelstelling overleg te organiseren tussen de verschillende betrokken partijen, teneinde op deze manier de veiligheidsconsulenten nauwer te betrekken bij de werkzaamheden van het OCMW.

De personen waarop deze procedures betrekking hebben, zijn de leden van de informaticadienst, de adviseur voor preventie en bescherming op het werk, de informatieveiligheidsadviseur evenals de dienst die de gegevens beheert.
In deze context speelt de persoon die is belast met het dagelijks bestuur, een beslissende rol in die mate dat hij/zij de deelname en integratie van zijn/haar veiligheidsconsulent in de verschillende structuren van de organisatie van het OCMW moet bevorderen.
Indien de veiligheidsconsulent niet integraal deel uitmaakt van het OCMW of slechts periodiek aanwezig is, is het belangrijk dat de persoon die is belast met het dagelijks bestuur, erover waakt dat de verschillende betrokken personen en de consulent op de hoogte worden gehouden.

Concreet en bij wijze van voorbeeld vermelden we het instellen van mondelinge of schriftelijke procedures om het overleg te garanderen met de verschillende betrokken diensten, teneinde de veiligheidsconsulent nauwer te betrekken bij de werking van het OCMW (overleg met de informaticadienst, de dienst voor gegevensbeheer, de dienst voor preventie en bescherming op het werk,...). Indien de veiligheidsconsulent slechts periodiek aanwezig is, is het hoofdzakelijk de persoon die is belast met het dagelijks bestuur van het OCMW die waakt over de organisatie van een communicatiekanaal.

Voorbeeld van een procedure: er werd een veiligheidsconsulent benoemd in het kader van een vereniging van vijf OCMW's. Er werd overeengekomen dat hij één voormiddag per maand in elk OCMW doorbrengt. Elke gebruiker van de vereniging beschikt over het werkschema van de consulent en de gegevens om hem te bereiken. Als een gebruiker dus zijn paswoord vergeet, contacteert hij de veiligheidsconsulent die eventueel op basis van het contract afgesloten met de informaticaleverancier van het betrokken OCMW, hetzij aan de informaticus van het OCMW hetzij aan de technicus van het informaticabedrijf vraagt confidentieel een nieuwe toegang te verlenen aan de werknemer. De gebruiker is verplicht een schriftelijke of elektronische aanvraag aan de consulent te richten om de interventie te kunnen traceren.

Het is tevens interessant voor de veiligheidsconsulent om een register bij te houden van incidenten die zich in de loop van het jaar hebben voorgedaan. Dit register kan worden bijgehouden in een schrift of op PC en dient idealiter de volgende informatie te bevatten:

Datum van het incident	Naam van de persoon die het incident heeft vastgesteld	Oorsprong, aard van het incident en gevolgen	Gegeven antwoord en te nemen voorzorgsmaatregel	Datum van oplossing	Naam van de persoon die het incident heeft opgelost
12/10/2005	Mevr. J. Dethiers	Virus in een bestand. Netwerk en PC's 2 u. lang geblokkeerd.	Scanning van de server met een noodupdate-CD, onderdrukken van het virus en herstarten van de server.	13/10/2005	Dhr. J. Secure, informaticus.

Tabel 1

Dit soort register is zeer nuttig want het maakt het mogelijk:

- de problemen die zich gedurende de referentieperiode (1 jaar) hebben voorgedaan, na te trekken;
- te kiezen welke stappen men onderneemt om de problemen op te lossen;
- eventueel de financiële verliezen en tijdverlies te evalueren, veroorzaakt door de incidenten en dus beter het belang kunnen beoordelen van de investering om te voorkomen dat het probleem of de problemen zich herhalen;
- sneller en preventief tussenbeide te komen om incidenten te vermijden.

4.2.2 Fysieke beveiliging en beveiliging van de omgeving.

Norm 4.2.2.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten, zowel tijdens als buiten de werkuren.

De informatieveiligheidsconsulent waakt erover dat de toegang tot het gebouw en de lokalen van het OCMW beperkt wordt tot de geautoriseerde personen.
Om een competent advies terzake te verstrekken, moet hij absoluut de toegang (zowel tot het gebouw als tot de lokalen) inventariseren evenals de verschillende categorieën van personen (bijv.: personeel, bezoekers, technici) die toegang hebben tot welke lokalen, onder welke omstandigheden, op welk ogenblik en onder welk toezicht. (bijv.: de toegang tot het serverlokaal beperken tot de personen van de dienst, bezoekers ontvangen in een speciaal daartoe voorzien lokaal, achter een balie, de gevoelige lokalen afsluiten buiten de werkuren, …).

Net als voor alle veiligheidsmaatregelen moeten de in het plan voorgestelde maatregelen beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

Deze toegangsbeperking moet worden georganiseerd volgens de omvang van het OCMW en de inrichting van de lokalen, bijvoorbeeld: automatische controle (badge en lezer), fysieke controle (onthaalbeambte).
De toegangscontrole kan zich tevens op een andere plaats bevinden die strategisch minder geschikt wordt bevonden (bijv.: ter hoogte van de toegang tot het gebouw of tot de lokalen van het OCMW). In de kleine OCMW's kan het eenvoudigweg gaan om een wachtruimte gereserveerd voor de bezoekers.

In elk geval moet men trachten te voorkomen dat personen met slechte bedoelingen makkelijk toegang hebben tot:
- het informaticamateriaal om het te vernielen/stelen en/of vertrouwelijke gegevens te raadplegen/aan te passen/vernietigen (bijv.: sociale gegevens van persoonlijke aard);
- de dossiers die sociale gegevens bevatten;
- de lokalen die archieven met vertrouwelijke gegevens bevatten.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Werkwijzen.

De server plaatsen in een lokaal waar het publiek geen toegang toe heeft en waar zo weinig mogelijk mensen voorbijkomen; dit lokaal moet op slot worden gedaan.

Bijvoorbeeld:

- *het kantoor van de Secretaris, een kamer zonder venster, een bureel van de administratieve dienst, enz. Zijn daarentegen te vermijden: de receptie, het kantoor waar de permanenties plaatsvinden,*

de Raadzaal, enz. Als het kantoor van de secretaris echter te klein is en het om technische redenen niet mogelijk is de server elders te plaatsen, moet de server worden geplaatst in een metalen kast die stevig aan de muur is bevestigd en voorzien is van onmisbare verluchtingsgaten voor de afkoeling van het toestel. Dit soort kast kan makkelijk door een gemeentearbeider worden gemaakt tegen een minimale prijs.

Toegangscontrole in het hele gebouw met behulp van registratieapparatuur.

Voorbeelden van toegangscontrole:

- *sommige OCMW's hebben aan de ingang van het gebouw een onthaalsysteem geïnstalleerd (bijvoorbeeld een wachtzaal) om ongewenste circulatie in het OCMW zo goed mogelijk te vermijden. Andere hebben er een alarmsysteem aan toegevoegd om de toegang tot het gebouw buiten de werkuren te controleren;*
- *sommige OCMW's gebruiken badge-systemen die toegang verlenen tot bepaalde lokalen gereserveerd voor de bevoegde personen. Opmerking: het is mogelijk één enkele badge-lezer te installeren voor één enkel lokaal maar de ingangen voor elke persoon te controleren. Het voordeel hiervan is de beperkte investering;*
- *het gebruik van sleutels en passe-partouts van de zogenaamde "gevoelige" lokalen beveiligen. Een systeem met een numeriek toetsenbord maakt het tevens mogelijk de toegang te beperken tot de bevoegde personen. Dit soort systeem kost minder dan 100 € exclusief installatie (makkelijk te installeren systeem);*

Norm 4.2.2.2. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet maatregelen treffen met betrekking tot de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade.

De veiligheidsmaatregelen tegen brand maken deel uit van het takenpakket van de preventieadviseur. De meer specifieke bescherming van het informaticamateriaal zal over het algemeen afhangen van de (grote) waarde ervan. In elk geval kunnen deze maatregelen (preventie, detectie, blussen) worden voorgesteld in samenwerking met de preventieadviseur en de erkende gespecialiseerde firma's. Het kan bijvoorbeeld gaan om de installatie van een branddetectie (detector, alarmcentrale) en een manueel (draagbare brandblussers) of automatisch brandblussysteem.

Wat de maatregelen tegen een eventuele inbraak betreft, zou het kunnen gaan om het op slot doen van de lokalen/gebouwen buiten de werkuren en/of de installatie van detectoren en een alarmcentrale en/of de organisatie van een fysieke bewaking door een bewakingsfirma of dergelijke.
De veiligheid verbeteren met behulp van eenvoudige hulpmiddelen: schermen die PC's verbergen en flatscreens, plaatjes die aangeven dat de lokalen beschermd zijn door een antidiefstalsysteem, de installatie van een webcam, de installatie van een valse camera (opgelet, het personeel en de bezoekers moeten worden verwittigd van de aanwezigheid van camera's).

Wat de veiligheidsmaatregelen tegen waterschade betreft, en alvorens maatregelen voor te stellen, zal men de bedreigingen moeten identificeren en bestuderen. Zo zal men bijvoorbeeld de voorkeur geven aan de installatie van informaticamateriaal op een verdieping in plaats van op de begane grond, ver van eventuele doorstroming van water,...). Opmerking: de informaticalokalen uitgerust met een airconditioning, moeten leidingen hebben voor de afvoer van condensatiewater. Let erop dat er geen waterbuizen boven de server of grote computers (mainframe) doorlopen.

Over het algemeen zijn een bepaald aantal actoren vaak bereid om u gratis te helpen en raad te geven: brandweer, specialisten van de gemeente, politie, intercommunales voor gas en elektriciteit, preventieambtenaar van de gemeente, enz…

Werkwijzen.

Plaats servers en PC's niet onder waterleidingen, op de grond, naast een koffieautomaat, een raam of een toegang tot het gebouw. Anderzijds is het belangrijk dat de server niet wordt blootgesteld aan extreme temperaturen; let er dus op dat hij wordt beschermd door een ventilatie- of klimaatregelingssysteem of in een geïsoleerde ruimte wordt geplaatst. Om de temperaturen te meten waaraan de toestellen worden blootgesteld, installeert u een thermometer uitgerust met een systeem dat de maximum- en minimumtemperaturen registreert (gewone en goedkope thermometer). In principe mag de temperatuur in het informaticalokaal 23° niet overschrijden (aanbeveling van HP).

Opgelet voor OCMW's in de buurt van een waterloop en voor overstromingsrisico's. Let er altijd op dat uw servers niet op de grond worden geplaatst en minstens een twintigtal centimeter boven de grond staan. Deze voorzorgsmaatregel geldt tevens voor de archieven en elektrische draden en kabels.

Opgelet voor OCMW's met een verouderde elektrische installatie. Vaak zijn informaticatoestellen aangesloten met dezelfde dominostekker. In dit geval geldt een reëel risico op verhitting en een verhoogd brandgevaar.
Plaats, volgens dezelfde gedachtegang, een brandblusser in de buurt van uw server, bij voorkeur buiten het informaticalokaal, aan de ingang bijvoorbeeld. Uw brandblusser moet niet alleen de

server kunnen blussen, maar ook de (tot een strikt minimum beperkte) documenten die in de buurt worden bewaard om de informaticus te helpen. Berg geen brandbaar materiaal op in de buurt van de server.
Installeer bij voorkeur geen automatisch blussysteem met water. Enkel sommige grote computers zijn bestand tegen waterverstuiving.

Overweeg uw informaticamateriaal te kunnen vervangen in geval van ramp en vooral als uw materiaal belangrijk is. Sommige informaticabedrijven of zelfs uw leverancier van sociale software kunnen zich er contractueel toe verbinden uw materiaal te vervangen en uw back-upgegevens opnieuw te installeren binnen een termijn die u samen met hen bepaalt.

Vermijd tevens:

- *uw informaticamateriaal te installeren in een lokaal met oriëntatie op het zuiden;*
- *een airconditioning te installeren als de temperatuur van uw lokaal nooit 23° overschrijdt;*
- *stopcontacten in de vloer (risico op kortsluiting);*
- *valse plafonds in contact met andere niet beschermde ruimtes.*

Verkies:

- *een depannagecontract binnen 24 u voor uw airconditioning (die makkelijker in panne zal vallen wanneer ze intensief draait en wanneer de leverancier nog vele andere aanvragen krijgt);*
- *de installatie van uw stopcontacten op minstens een tiental centimeters van de vloer.*

Norm 4.3.3. **het OCMW moet over een alternatieve stroomvoorziening beschikken waardoor de informaticaverwerkingen zonder risico kunnen worden afgesloten (voor de instellingen die een secundair netwerk beheren en/of die gegevens leveren in het kader van de sociale zekerheid).**

Informaticatoestellen zijn vrij gevoelig voor storingen in de stroomvoorziening (afsluiten, pieken of onevenwichtige spanning, …).
Het risico dat het OCMW loopt bij gebrek aan een alternatieve stroomvoorziening, berust in het verlies van het werk dat op dat ogenblik wordt uitgevoerd: de werknemer zal de gegevens opnieuw moeten beginnen invoeren zonder per se te weten welke gegevens werden doorgestuurd of niet. De duur van de autonome stroomvoorziening die noodzakelijk is in geval van een elektriciteitspanne om een uitwisseling van gegevens mogelijk te maken, wordt geschat op ongeveer een half uur.
Zonder daarom aanzienlijke financiële middelen in te zetten, kan men vandaag investeren in oplossingen waarmee men de verplichtingen kan nakomen die in deze norm worden geformuleerd. De consulent die geen informatie heeft over dit onderwerp, kan contact opnemen met zijn voogdij-administratie of, bij gebrek hieraan, met één van de partners opgesomd aan het eind van deze handleiding.

Wat de hulp- en noodvoorziening betreft (een elektriciteitsgenerator bijvoorbeeld), deze hebben tot doel een ononderbroken stroomvoorziening te garanderen en de kwaliteit van de stroombron te verbeteren. Ze zijn helaas erg duur. Om u te helpen bij uw keuze van toestellen raden wij u aan zich te richten tot de vertegenwoordiger van uw leverancier van informaticamateriaal. Bij wijze van voorbeeld signaleren wij dat er heel wat materiaal op de markt is dat de beveiliging van de stroomvoorziening van één of meer PC's/servers of van uw hele informaticasysteem kan verzekeren zoals onderandere een noodgroep, gelijkrichters met accubatterij en alternator (er zijn reeds UPS-systemen beschikbaar vanaf 250 €) met of zonder noodgroep (motor).

Net als voor alle veiligheidsmaatregelen moet alle nodige materiaal om te beschikken over een alternatieve stroomvoorziening die het mogelijk maakt de informaticaverwerkingen zonder risico af te sluiten, beantwoorden aan de specifieke behoeften van elk OCMW.

Opgelet: sluit enkel het strikt noodzakelijke aan opdat een UPS erin zal slagen de server van stroom te voorzien, zodat deze zijn activiteiten kan afsluiten zonder verlies van gegevens. Zo niet zal uw UPS die slechts van een batterij is voorzien, niet voldoende stroom kunnen leveren en gaan uw gegevens verloren.

4.2.3 Logische toegangsbeveiliging.

Norm 4.2.3.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet de toegang tot de gegevens die nodig zijn voor de toepassing en de uitvoering van de sociale zekerheid, beveiligen door middel van een identificatie-, authentificatie- en autorisatiesysteem.

Hier zijn enkele voorafgaande definities nodig:
Identificatie.
Gegevens ingevoerd door de gebruiker waardoor het informaticasysteem hem kan identificeren (bijv.: naam en/of voornaam, controlenummer, Userid, …).

Authentificatie.
Gegeven (wachtwoord) ingevoerd door de gebruiker waardoor het informaticasysteem zich ervan kan vergewissen dat de gebruiker wel degelijk de persoon is die hij beweert te zijn (geheime code, chipkaart, biometrische gegevens, elektronisch token…).
Gelieve regelmatig van wachtwoord te veranderen en ervoor te zorgen dat enkel de gebruiker zelf het kent.

Opgelet: laat geen wachtwoorden circuleren of kleef geen post-it met het wachtwoord erop als geheugensteuntje op uw scherm. U kan tips vinden op de website van de POD MI: http://www.mi-is.be/Nl/content/goedbeheerpaswoord.pdf.

Autorisatie.
De toegang van de gebruikers beperken tot de gegevens, dienst, toepassingen, ... die noodzakelijk zijn voor het uitvoeren van hun taken (bijv.:het opstellen van gebruikersprofielen: wie toegang heeft tot wat in de softwarepaketten, reserveer de toegang tot de toepassingen van de sociale zekerheid tot één of meer personeelsleden van het OCMW,...)

De informatieveiligheidsconsulent moet erover waken dat er zulke een systeem van toegangsbeveiliging in voege is. Dit kan met of zonder samenwerking met de persoon die is belast met het dagelijks bestuur van het informaticasysteem.

Waarschijnlijk zal in de toekomst een ambtenaarstoken of de elektronische identiteitskaart worden veralgemeend in het toegangsproces tot het portaal van de sociale zekerheid (dat is reeds het geval voor de federale portaal).
In deze context is een POLICY die de strenge regels bepaalt, beschikbaar op de website van de KSZ op: http://ksz-bcss.fgov.be/documentation/nl/News/ambtenaartoken.pdf

Net als voor alle veiligheidsmaatregelen, moeten de maatregelen om de toegang te beveiligen tot de gegevens die noodzakelijk zijn voor de toepassing en de uitvoering van de sociale zekerheid door middel van een identificatie-, authentificatie- en autorisatiesysteem *beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.*

Norm 4.2.3.2. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een loggingsysteem implementeren voor de persoonsgegevens die nodig zijn voor de toepassing en uitvoering van de sociale zekerheid.

Algemene regels.

Definitie van ‘‘Logging’’: historische gegevens (wie heeft wat gedaan en wanneer) waarmee men, a posteriori, de gebruiker, de behandelde gegevens / toepassing evenals de data/uren van de bewerking kan identificeren.

Bijvoorbeeld: de veiligheidsconsulent moet in staat zijn terug te vinden welke maatschappelijk werker de gegevens van het nationaal register heeft geraadpleegd via een elektronische verbinding met de KSZ op vrijdag 11 juni om 11.43 u. of welke administratieve ambtenaar een dossier heeft ingegeven op 10 juni in de sociale software.

Het log of de logging is dus een opname, een spoor van een uitgevoerde verwerking. Afhankelijk van het gevraagde niveau kunnen alle uitgevoerde verwerkingen worden opgevraagd.
Enkel uw leverancier van sociale software zal in staat zijn dit systeem op uw sociale programma te installeren (verscheidene leveranciers van sociale software beschikken over dit systeem dat soms reeds geïnstalleerd is). Wat uw informatica-omgeving betreft (Windows 98, 2000, XP, Linux, AS400, enz.) en als dat nodig blijkt, zijn er producten beschikbaar op de markt of in open source (openbare informaticacode).

De veiligheidsconsulent moet tevens anticiperen op de verscheidene problemen in verband met de loggings, samen met de verantwoordelijke voor het dagelijks bestuur en de informaticus als het OCMW er een heeft:

- wat gaan we opnemen in de loggings? Enkel de naam van de gebruikers of hun identificatie, de data en uren, de betrokken programma's en toepassingen evenals de aard van de wijziging of gaan we ook de wijziging zelf en andere inlichtingen opnemen? In dat geval heeft men veel geheugen nodig om alles te bewaren;
- hoe lang gaan we de loggings bewaren? Zal de bewaartijd worden bepaald op basis van de uiterste datum voor het opsporen van een opzettelijke fout (6 maanden) of langer afhankelijk van de aard van de inbreuk?
- op welke dragers zullen de loggings worden bewaard? Op diskettes met een soms wisselvallige werking, op CD's waarvan de toekomst onzeker lijkt, op DVD's, op banden? Vergeet niet dat alle informaticadragers een beperkte levensduur hebben (een honderdtal keer gebruik van de banden volgens bepaalde leveranciers);
- waar zullen we de loggings bewaren? Wie zal toegang hebben tot de loggings en volgens welke procedure?
- zullen we er zeker van zijn dat de loggings niet kunnen worden gewijzigd of gemanipuleerd?

Op al deze vragen kunt u een antwoord vinden en uw informaticaleverancier kan u hierbij helpen.

Werkwijzen.
Een goede logging zal geen tijdverlies betekenen. Ze moet u namelijk in staat stellen te reageren per afwijking:

Voorbeelden:

- *overzicht van een abnormaal hoog aantal raadplegingen door een gebruiker;*
- *herhaaldelijke en vruchteloze pogingen om verbinding te maken met een programma zonder autorisatie;*
- *overzicht van een abnormaal hoog aantal kopieën van gegevens of van schermen;*
- *poging tot verbinding onder een andere identiteit;*
- *aantal wijzigingen aangebracht aan een dossier dat het door de dienst vooropgestelde aantal overschrijdt;*
- *enz.*

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Norm 4.2.3.3. **elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een systeem van regelmatig te controleren veiligheidskopieën (back-up) invoeren om, in geval van beperkte of totale ramp, elk onherstelbaar verlies van gegevens te voorkomen (gegevens nodig voor de toepassing en de uitvoering van de sociale zekerheid alsook de gegevens met betrekking tot de toepassingen en het besturingssysteem).**

Het is in nauwe samenwerking met de perso(o)n(en) die is/zijn belast met het beheer van het informaticasysteem, dat de informatieveiligheidsconsulent van het OCMW zal kunnen waken over de verwezenlijking van deze opdracht. Het gaat erom, zowel voor de gegevens die nodig zijn voor de toepassing en de uitvoering van de sociale zekerheid als voor deze met betrekking tot de toepassingen en het besturingssysteem, een systeem in te voeren van regelmatig te controleren veiligheidskopieën (1). Deze veiligheidskopieën moeten elk onherstelbaar verlies van gegevens voorkomen in geval van beperkte of totale ramp.
Om de veiligheid van de back-ups te garanderen moet een exemplaar ervan elders worden bewaard.
De veiligheidsconsulent waakt erover dat hij van de informaticateams een document krijgt waarin de back-up- en de eraan verbonden herstelprocedures staan beschreven.
Deze documenten worden afgedrukt en eveneens elders bewaard.

Het back-upsysteem van de gegevens is noodzakelijk om een onherstelbaar verlies ten gevolge van een ongeval te voorkomen. Dankzij deze back-up moet het OCMW zijn activiteiten opnieuw kunnen opstarten na een incident dat het systeem ter plaatse heeft vernietigd.
Om een back-up te maken, volstaat het de gegevens op te slaan op een CD-rom, een DVD, een magneetband, enz. en deze opname op te bergen. De back-up van gegevens moet automatisch en regelmatig, idealiter dagelijks, plaatsvinden.

Idealiter zou het goed zijn dagelijks een back-up te maken van de gewijzigde gegevens van de dag en dit van maandag tot donderdag. Op vrijdag wordt een volledige back-up van de gegevens en de informatica-configuratie gedaan.
Deze volledige back-up moet wekelijks worden gedaan op een andere band gedurende vijf weken om zo een maand te kunnen dekken. Dankzij dit systeem kunnen de historische betalingsgegevens die eventueel nuttig zijn voor het OCMW, worden bewaard.

Onderstaand schema legt uit hoe de back-ups idealiter zouden moeten worden uitgevoerd:

Dag		**Week 1**		**Week 2**		**Week 3**		**Week 4**		**Week 5**		**Week 1**
Maandag	B1	Dagelijkse back-up	S5	Dagelijkse back-up	B1	Dagelijkse back-up	B5	Dagelijkse back-up	B1	Dagelijkse back-up	B5	Dagelijkse back-up
Dinsdag	B2	Dagelijkse back-up	S6	Dagelijkse back-up	B2	Dagelijkse back-up	B6	Dagelijkse back-up	B2	Dagelijkse back-up	B6	Dagelijkse back-up
Woensd.	B3	Dagelijkse back-up	S7	Dagelijkse back-up	B3	Dagelijkse back-up	B7	Dagelijkse back-up	B3	Dagelijkse back-up	B7	Dagelijkse back-up
Donderd.	B4	Dagelijkse back-up	S8	Dagelijkse back-up	B4	Dagelijkse back-up	B8	Dagelijkse back-up	B4	Dagelijkse back-up	B8	Dagelijkse back-up
Vrijdag	T1	Totale back-up	T2	Totale back-up	T3	Totale back-up	T4	Totale back-up	T5	Totale back-up	T1	Totale back-up

Tabel 2.

Uitleg: de maandag van de eerste week dient band B1 uitsluitend voor de back-up van gegevens die deze maandag zijn gewijzigd. Hetzelfde geldt tot donderdag.

De vrijdag van week 1 wordt een totale back-up T1 (volledige gegevens en systeem) uitgevoerd. Deze back-upband wordt buiten het OCMW bewaard.
Week 2 wordt hetzelfde proces herhaald. Elke dag wordt een andere band gebruikt.

Er zullen dus 8 banden voor de dagelijkse back-up zijn die over twee weken worden gebruikt. De cyclus herhaalt zich dus om de twee weken.
Wat de wekelijkse back-ups betreft, de complete back-ups (informatica-omgeving en gegevens), deze worden gespreid over 5 weken. Er zullen bijgevolg 5 banden zijn (of meer als de back-up meer banden vergt) verspreid over een maand.

(1) In zijn jaarlijkse veiligheidsplan moet de consulent minstens één keer per jaar in een restore-test voorzien van het hele of het gedeeltelijke informaticasysteem vanaf de dragers van de back-ups.

De back-upcyclus moet worden beslist door de persoon die is belast met het dagelijks bestuur, na overleg met alle betrokken partijen: informatici, leverancier, veiligheidsconsulent en verantwoordelijke voor de interne diensten.
Tijdens dit overleg is het goed de maximaal toelaatbare duur van de gegevens te bepalen. Zo moet de verantwoordelijke voor het dagelijks bestuur, als men de dagelijkse gegevens op het OCMW zelf bewaart, bereid zijn het verlies van 4 dagen gegevens, dat wil zeggen 4 dagen werk, te aanvaarden. Als de wekelijkse back-up ter plaatse wordt bewaard dan worden, in geval van een grote ramp, alle gegevens vernietigd en zal het onmogelijk zijn voor het OCMW om welke gegevens dan ook te recupereren.

AANBEVELINGEN INZAKE BACK-UPS

1. Algemeen

Op het gebied van organisatie is het meestal beter de informatie niet op een PC op te slaan. Op het gebied van vertrouwelijkheid is er altijd het risico op diefstal van de PC en wat de beschikbaarheid betreft, worden de back-ups regelmatiger en systematisch verzekerd door de informatica.
De back-ups zijn noodexemplaren die op korte termijn worden bewaard om de effecten van een ongeval, meestal op informaticagebied, tot een minimum te beperken en om deze gegevens of bestanden te kunnen herstellen in een toestand die dicht aanleunt bij hun laatst gekende toestand.
De archieven zijn exemplaren van bestanden die op lange termijn worden bewaard om er een spoor van te bewaren in een gegeven toestand.
Uit deze definities komt voort dat de doelstellingen niet dezelfde zijn en dat de informatici moeten beschikken over precieze regels die zijn goedgekeurd door de verantwoordelijke van de organisatie, de verantwoordelijke van de toepassing en de informaticaverantwoordelijke.
De verantwoordelijkheid voor de plaatselijk bewaarde back-ups van gegevens (op de schijf van de PC of het station) valt onder de verantwoordelijkheid van elke gebruiker.
Voor de aangesloten posten wordt een kopie door een server aanbevolen, in de mate waarin back-ups worden uitgevoerd door de administrator van de server en beveiligd opgeslagen.
Is dat niet mogelijk, dan is het aanbevolen de back-ups op te bergen in een andere plaats dan degene waar de werkpost (PC) zich bevindt.
De lokalen waar de back-ups en archieven worden opgeslagen, moeten worden beschermd.
De frequenties en de vereisten voor de back-ups en het herstel moeten worden gedefinieerd.
De loggings maken het onderwerp uit van een systematische dagelijkse back-up.

2. Back-upplannen van de basissoftware en de systemen

De back-ups van de configuraties worden buiten de productiesite bewaard.
Er moet een procedure worden ingesteld waardoor men kan garanderen dat men met de back-up van de configuraties op elk moment de productie-omgeving kan herstellen.

2. Back-upplannen voor toepassingsgegevens

Zie tabel 2 van de back-ups op pagina 28.

De back-ups moeten genomen worden in functie van de risico's.

Het back-upplan moet bij elke verandering in de besturingscontext worden bijgewerkt en meer in het bijzonder bij elke creatie of wijziging van toepassingen.
Men moet regelmatig nagaan of een herneming of het herstarten effectief mogelijk is vanaf de gemaakte back-ups (onverwachtse integriteitstest in werkelijkheid).

4. Back-uptests.
Er bestaan systemen waarmee u de geldigheid van de back-up kunt testen:
- *herlezen van een deel van de gegevens op de back-upband door het systeem;*
- *opnieuw installeren van een steekproef uit de gegevens om ze te herlezen en hun geldigheid na te gaan.*

Als het systeem weergeeft : "De back-up is goed verlopen", dan betekent dat niet dat de gegevens herbruikbaar zijn. Vergewis u ervan dat een doeltreffend testsysteem de herbruikbaarheid van de gegevens garandeert. Uw leverancier kan u hierbij nuttige raad geven.

Net zoals voor alle veiligheidsmaatregelen moeten de installatie van de back-ups en hun procedures beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

Norm 4.2.3.4. **elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een systeem en formele**, **geactualiseerde procedures installeren die het mogelijk maken om veiligheidsinbreuken te detecteren, op te volgen en te herstellen.**

Elke inbreuk op de veiligheid wijst op een zwakte in de geïnstalleerde mechanismen. Het is zeer belangrijk dat deze incidenten worden geïnventariseerd en tot doeltreffende corrigerende maatregelen leiden.
Voorzorgsmaatregelen zijn essentieel in deze context, met name door:

- de ontwikkeling van een streng beleid op het gebied van toegang tot het informatiesysteem (wie heeft recht op wat) ;
- strenge regels voor het definiëren van een gebruikerscode en het paswoord;
- streng toepassen van de frequentie waarmee paswoorden worden gewijzigd;
- de toepassing van een gedragscode op het gebied van e-mail en internet;
- het instellen en publiceren van een procedure te volgen in geval van virusinfecties;
- het updaten van de antivirusprogramma's en firewalls;
- het abonnement (vaak gratis) op deskundige centra op het gebied van informatie over de evolutie van aanvallen tegen netwerken;

In geval van een incident kan een formele procedure een eenvoudig document zijn dat aan de verantwoordelijke voor het dagelijks bestuur wordt overhandigd en, naargelang het type van incident, wordt opgesteld door de verschillende verantwoordelijken of betrokkenen binnen de organisatie.

Deze procedure moet idealiter de volgende elementen bevatten:

- de beschrijving van de inbreuk of van het incident;
- de origine of oorzaak van de inbreuk of het incident;
- de gevolgen voor de organisatie of het netwerk van de sociale zekerheid;
- de ondernomen stappen om de problemen op te lossen;
- de personen die zijn tussenbeide gekomen om de problemen op te lossen;
- de te nemen maatregelen om de gevolgen van de inbreuk of het incident tot een minimum te beperken.

Zie Tabel 1 bladzijde 18.
De consulent moet erop toezien dat de nodige corrigerende maatregelen worden genomen.

Net als voor alle veiligheidsmaatregelen moet het installeren van een systeem en formele, geactualiseerde procedures die het mogelijk maken veiligheidsinbreuken te detecteren, op te volgen en te herstellen, beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Norm 4.2.3.5. **wanneer de OCMW's die in APPC-modus (gestructureerde mededeling) zijn aangesloten op de Kruispuntbank, in de zone "USERID" van het prefixgedeelte van een bericht aan de Kruispuntbank, het programmanummer overnemen dat aan de basis ligt van het bericht dat ze naar de Kruispuntbank sturen, alhoewel een natuurlijk persoon aan de oorsprong van het bericht ligt, kan de Kruispuntbank, a posteriori, het programmanummer terugvinden. De Kruispuntbank kent echter de identiteit niet van de natuurlijke persoon die het bericht verstuurde.**

In dat geval moet het OCMW dus zelf de link leggen tussen het programmanummer dat het overneemt in het prefixgedeelte van het bericht dat het naar de Kruispuntbank stuurt, en de identiteit van de natuurlijke persoon die het bericht verstuurt.

Om het verband te leggen tussen de natuurlijke persoon en de opvraging moet het OCMW de loggings raadplegen zoals gespecifieerd in de norm 4.2.3.2.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

4.2.4 Ontwikkeling, productie en maintenance van toepassingen.

Norm 4.2.4.1. **elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over formele en geactualiseerde procedures beschikken voor het in productie stellen van nieuwe toepassingen en het aanpassen van bestaande toepassingen, teneinde te voorkomen dat een enkele persoon alleen de controle zou verwerven over dit proces.**

Het aanpassen van bestaande toepassingen en het in productie stellen van nieuwe toepassingen moet steeds vooraf worden getest. Idealiter worden deze tests uitgevoerd in een omgeving buiten de productie-omgeving (een omgeving gewijd aan het uitvoeren van tests op fictieve gegevens).
Het testen en vervolgens het in productie stellen van een toepassing moet idealiter door een andere persoon gebeuren. Deze procedure zal vervolgens worden geformaliseerd en aangepast afhankelijk van de behoefte.
In geval van het in productie stellen van een nieuwe versie voor een bestaande toepassing moet in de procedure in een back-up worden voorzien van de huidige versie en haar onderdelen alvorens de nieuwe versie wordt geïnstalleerd en dit om slecht functioneren te voorkomen en te kunnen terugvallen op de vorige versie.

Opgelet: dit geldt enkel voor ontwikkelaars van toepassingen. De OCMW's zijn vrij om aan hun softwareleveranciers te vragen om deze veiligheidsnormen te respecteren.

Norm 4.2.4.2. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over formele en geactualiseerde procedures beschikken voor de uitwerking van documentatie bij de ontwikkeling van nieuwe toepassingen en systempen en het onderhoud van bestaande toepassingen en systemen.

Voor de OCMW's die hun toepassingen en systemen zelf ontwikkelen en actualiseren, is het nuttig documentatie uit te werken. Deze documentatie kan de ontwikkeling ervan en de aangebrachte wijzigingen preciseren en zal het mogelijk maken, a posteriori, de organisatie ervan te kennen.
Bij de installatie van nieuwe toepassingen moet men tevens toezien op de documentatie/opleiding van de gebruikers, op de back-upprocedures, op de toegangscontroles tot de toepassing, op de aanwezigheid, indien nodig, van gebruiksloggings en op de integratie van deze toepassing in het algemene noodplan.
Deze procedure zal vervolgens worden geformaliseerd en aangepast afhankelijk van de behoefte.

Net zoals voor alle veiligheidsmaatregelen moeten het beschikken over formele en geactualiseerde procedures voor de uitwerking van documentatie bij de ontwikkeling van nieuwe toepassingen en systemen en het onderhoud van bestaande toepassingen en systemen beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Opgelet: dit geldt enkel voor ontwikkelaars van toepassingen. De OCMW's zijn vrij om aan hun softwareleveranciers te vragen om deze veiligheidsnormen te respecteren.

4.2.5 Netwerkbeveiliging.

Norm 4.2.5.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet de toegang tot het (de) informaticasyste(e)m(en) beperken tot geïdentificeerde, geauthentifieerde en geautoriseerde personen/objecten.

Onder “informaticasysteem” verstaan we de toestellen en computers die worden gebruikt voor de verwerking van gegevens. Deze minimale veiligheidsnorm nodigt de OCMW’s, afhankelijk van de omvang van hun organisatie, uit om hun informaticasystemen te beveiligen tegen kwaadwilligheid en/of diefstal door beschermende maatregelen te treffen.

Deze maatregelen kunnen bij voorbeeld als volgt worden opgesomd (lijst niet exhaustief):

- geen informaticamateriaal onbeheerd achterlaten;
- bepaalde belangrijke toestellen in een beveiligd lokaal plaatsen;
- de vrije toegang buiten de werkuren verbieden (bijv.: kantoor op slot, systeem voor toegangscontrole, inbraakdetectie,...);
- de schermen vergrendelen of de activering van de screen saver verplichten;
- een identificatie-, authentificatie- en autorisatiesysteem opleggen voor toegang tot het netwerk;
- de informaticadragers op een beveiligde plaats bewaren;
- geen afgedrukte documenten met vertrouwelijke informatie laten rondslingeren;
- procedures instellen voor de begeleiding en opvolging tijdens bezoeken van de leveranciers van informaticadiensten of andere;
- de wachtwoorden van de system administrators wijzigen na tussenkomst van externe technische diensten;
- veiligheidsregels instellen en laten toepassen tegenover de leveranciers van diensten. (Policy beschikbaar op de website van de KSZ).
- de toegang vanop afstand (teleworking / homeworking) moet aan strenge maatregelen onderworpen zijn. Policy’s op de website van de KSZ preciseren de regels terzake. Wij raden de bij dit gebruik betrokken OCMW’s aan contact op te nemen met de veiligheidsdienst van de POD MI die hen hierbij kan helpen.
- een gedragscode instellen voor het gebruik van e-mail en internet.

Net als voor alle veiligheidsmaatregelen, moeten de maatregelen om de toegang tot het (de) informaticasyste(e)m(en) te beperken tot geïdentificeerde, geauthentifieerde en geautoriseerde personen/objecten beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Norm 4.2.5.2. **elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een systeem en formele, geactualiseerde procedures installeren die het mogelijk maken om veiligheidsinbreuken te detecteren, op te volgen en te herstellen.**

- Zie norm 4.2.3.4 maar dan toegepast op het netwerk.

Norm 4.2.5.3. **de OCMW's kunnen voor hun aan de sociale zekerheid externe TCP/IP-verbindingen gebruik maken van het Extranet van de sociale zekerheid.**

Voor de rechtstreekse verbindingen met hun aan de sociale zekerheid externe TCP/IP-netwerken moeten de betrokken OCMW's veiligheidsmaatregelen implementeren die in overeenstemming zijn en blijven met de maatregelen die zijn getroffen op het niveau van het Extranet van de sociale zekerheid.

Deze norm is enkel van toepassing op de OCMW's die toegang willen hebben naar het internet via het extranet.

3.2.6. Continuïteitsplan.

Norm 4.2.6.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een risicoanalyse uitvoeren teneinde de opstelling van een continuïteitsplan mogelijk te maken.

Het continuïteitsplan is een document dat wordt opgesteld door de veiligheidsconsulent en tot doel heeft de stappen te bepalen en uiteen te zetten die moeten worden genomen in geval van een incident.

Bijvoorbeeld: hoe vind ik de verbinding en de gegevens terug nadat de server werd gestolen of vernield? Wat doen als u de wachtwoorden vergeet of verliest? Hoe reageren op een aanval van een computervirus?

Risicoanalyse

Dankzij een volledige inventaris van de goederen (gebouw, lokalen, materiaal, software, toepassingen...) en van de risico's die men loopt (vernieling, verlies, verduistering...) kan de veiligheidsconsulent weten waarover het OCMW moet beschikken om correct te kunnen werken.
In geval van een beperkte of totale ramp moet het OCMW trachten zo snel mogelijk opnieuw te beginnen te werken. In overleg tussen de veiligheidsconsulent en de verantwoordelijke voor het dagelijks bestuur van het OCMW zal een termijn worden bepaald. Het zou namelijk kunnen dat alle activiteiten niet prioritair zijn maar dat andere op zeer korte termijn moeten worden herstart.
De veiligheidsconsulent moet dan een risicoanalyse opstellen op basis van datgene waaraan het het OCMW zou ontbreken om te beantwoorden aan de vereisten om weer op te starten.
De gebreken zullen vooral uit informatie bestaan (wat is de procedure om de verbinding met Publilink opnieuw te maken, hoe beschikken we snel weer over een server om de activiteiten en betalingen weer op te starten? Hoe brengen we de telefoonlijnen terug in orde om vragen naar sociale hulp te beantwoorden? Waar kunnen we ons opnieuw installeren? Zullen we beschikken over de nodige telefoonlijnen en informatica? Enz.)
De risicoanalyse zal, afhankelijk van de omgeving van het OCMW (stedelijke of landelijke omgeving, lokalen beschikbaar of niet, hoge criminaliteitsgraad of niet) de klemtoon leggen op de meest waarschijnlijke risico's. De veiligheidsconsulent kan dan een continuïteitsplan voorstellen dat een gepast antwoord biedt op deze risico's.

Om dat te doen, moeten in de risicoanalyse in het bijzonder de volgende aspecten aan bod komen:

- **informaticagebonden rampen:** zijn alle logische of fysieke problemen die uitsluitend één of meer elementen van het informaticasysteem van het OCMW aanbelangen;
- **niet-informaticagebonden rampen buiten de kantooruren:** is de schade aan het gebouw, het personeel en het materieel ten gevolge van een natuurramp of een menselijke ramp.
- **niet-informaticagebonden schadegevallen tijdens de kantooruren:** is de schade veroorzaakt aan het gebouw, het personeel en het materiaal ten gevolge van een natuurramp of een menselijke ramp.
- **het migratieplan:** beschrijft het te volgen proces om het informaticasysteem opnieuw in werking te stellen en het personeel een werkomgeving te verschaffen. Het is belangrijk de rol te preciseren van elke bij dit proces betrokken speler om alles weer in werking te stellen.

Uiteraard moet niet alleen rekening worden gehouden met een totale ramp.

Norm 4.2.6.2. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een continuïteitsplan opstellen, testen en onderhouden teneinde de opdrachten betreffende sociale zekerheid van het OCMW te kunnen waarborgen. Tevens moet het in een informatica-uitwijkcentrum voorzien in geval van beperkte of totale ramp.

Rekening houdend met de scenario's van de risicoanalyse kan de veiligheidsconsulent, in nauwe samenwerking met alle actoren van zijn organisatie en zich inspirerend op de methodologie die is beschreven in het document "Gemeenschappelijke methodologie voor het uitwerken van een continuïteitsplan" dat werd opgesteld door de werkgroep "Informatieveiligheid", de nodige organisatorische en technische maatregelen uitwerken om een continuïteitsplan in te stellen.

Dit continuïteitsplan moet over het algemeen de volgende aspecten bevatten:

- **personeel:** adressen, telefoonnummers, andere personeelsgegevens, gegevens van de officiële instanties, van een crisiscomité belast met het nemen van beslissingen op basis van de evolutie van de situatie, van informaticaleveranciers en andere, van verzekeringsmaatschappijen, van artsen, van professionele partners, nuttige telefoonnummers...
- **technische middelen:** inventaris van het materiaal, van de formulieren en papieren dragers, van de hardware, de software, de structuur van het interne en externe informaticanetwerk, de toepassingen, het proces voor contacten met de pers, de partners...
- **plan voor de technische herstart:** beschrijving van alle etappes om het hele informaticasysteem opnieuw op te starten en te herstellen.

Indien zich een ramp voordoet, zal het OCMW er dankzij dit continuïteitsplan voor kunnen zorgen dat het binnen de kortste termijn weer kan opstarten en de continuïteit van de opdrachten betreffende sociale zekerheid van het OCMW waarborgen.

Om operationeel te blijven, zal het continuïteitsplan regelmatig worden getest en voortdurend worden bijgewerkt. De documentatie ervan zal buiten de instelling worden bewaard. (bvb.: de betrokken medewerkers bewaren een exemplaar thuis).
Er moet in procedures worden voorzien om in geval van schade over dit plan te kunnen beschikken.

Bijvoorbeeld: wat zou er gebeuren als de back-ups niet werken en ons informaticasysteem is vernield (overstroming bijvoorbeeld) ?

De norm 4.2.3.3 preciseert dat het OCMW maatregelen moet treffen om elk onherstelbaar verlies van gegevens te voorkomen. De veiligheidsconsulent stelt dus aan de verantwoordelijke voor het dagelijks bestuur maatregelen voor die het mogelijk maken deze norm na te leven.

Op basis van de punten die in de risicoanalyse aan bod komen, beschrijft de veiligheidsconsulent in het continuïteitsplan alle stappen die moeten worden ondernomen in geval van een incident. Het is belangrijk dat elke persoon die moet tussenbeide komen, op de hoogte is van de bepalingen van het continuïteitsplan, zodat zelfs in afwezigheid van de veiligheidsconsulent de verbinding snel weer kan worden hersteld. Het organisatorische gedeelte is dus zeer belangrijk. Wie doet wat, hoe en waar om een antwoord te bieden op het probleem en zijn rol te spelen?

We hernemen het voorbeeld dat we hierboven zijn begonnen: de vernietiging van de back-upgegevens en het informaticasysteem.

De veiligheidsconsulent zal dus één of meer van de volgende voorzorgsmaatregelen voorstellen:

- een testsysteem dat de geldigheid van de back-ups garandeert;
- een procedure die het aantal back-ups telt om de media waarop ze worden opgeslagen (CD, DVD, magneetbanden, andere) tijdig te vervangen en te voorkomen dat hun kwaliteit erop achteruitgaat;
- de back-ups toevertrouwen aan een externe leverancier;
- een dubbel van de back-ups maken;
- een systeem van harde schijven van het RAID-type aanschaffen;
- enz.

Wanneer men een oplossing heeft gekozen, moet men de functionaliteit ervan nagaan en ze testen, intern of met de leverancier. Ze zal dus bruikbaar zijn als deze ramp zich zou voordoen.
Natuurlijk zijn sommige risico's aanvaardbaar, maar alleen de verantwoordelijke voor het dagelijks bestuur kan hierover oordelen.
De vernietiging van een PC, die snel vervangbaar is, is een aanvaardbaar risico. Het faillissement van een leverancier kan heel wat erger zijn. Wat doen als deze verdwijnt? Wie gaat mijn programma verder onderhouden? Hoe kan ik hem vervangen? Hoe groot is het risico dat deze leverancier failliet gaat?
De veiligheidsconsulent kan een "escrow clause" in het contract met de leverancier laten opnemen. Dat houdt in dat de leverancier de bijgewerkte bronbestanden van zijn programma's onderbrengt bij een derde vertrouwenspersoon: kamer van koophandel, notaris, instelling of andere, zodat het OCMW deze kan recupereren en het onderhoud laten doen in afwachting van een andere oplossing.

Net als voor alle veiligheidsmaatregelen moeten de maatregelen om een continuïteitsplan op te stellen, te testen en te onderhouden om de opdrachten inzake sociale zekerheid van het OCMW te kunnen waarborgen en het voorzien van een informatica-uitwijkcentrum in geval van een ramp beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

4.2.6 Inventaris.

Norm 4.2.7.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over een permanent bijgewerkte inventaris beschikken van het informaticamateriaal en de software.

Om de heropbouw binnen de kortste termijn te verzekeren en zo de continuïteit van de opdrachten inzake sociale zekerheid van het OCMW te waarborgen, moet men een continuïteitsplan opstellen, testen en onderhouden. Om zijn continuïteitsplan te optimaliseren, zorgt de informatieveiligheidsconsulent er onder meer voor dat hij beschikt over een permanent bijgewerkte inventaris van het informaticamateriaal en software. Deze inventaris kan opgemaakt worden door middel van een programma. Voor meer informatie, gelieve de helpdesk van de POD MI te contacteren. De inventaris van de middelen die noodzakelijk zijn voor het uitvoeren van de taken van het OCMW, kan integraal deel uitmaken van het betrokken continuïteitsplan. Dankzij deze inventaris moet men, in geval van ramp, een zo snel mogelijke heropbouw van het informaticasysteem van het OCMW kunnen waarborgen.

Net als alle veiligheidsmaatregelen moeten de maatregelen om te beschikken over een permanent bijgewerkte inventaris van het informaticamateriaal en de software, beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

4.2.7 Bescherming tegen virusinfecties.

Norm 4.2.8.1. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet over een gebruikershandleiding beschikken met betrekking tot het voorkomen van virusbesmettingen, het gebruik van de geïnstalleerde antivirussoftware en de te ondernemen acties in geval van virusinfectie.

De informatieveiligheidsconsulent van het OCMW zorgt ervoor dat zijn gebruikers beschikken over een document (handleiding) met betrekking tot:

- voorzorgsmaatregelen die de gebruikers moeten naleven;
- de werking van de eventueel op de werkpost geïnstalleerde antivirussoftware;
- door de gebruiker te ondernemen acties in geval van een virusinfectie (bijvoorbeeld: de door een gebruiker te ondernemen actie kan zich soms beperken tot het niet openen van een verdacht e-mailbericht en de persoon die is belast met het beheer van het informaticasysteem verwittigen, of indien de PC geïnfecteerd is door een virus: de persoon die is belast met het beheer van het informaticasysteem verwittigen).

Om deze handleiding zo goed mogelijk uit te werken, is een nauwe samenwerking met de persoon die is belast voor het beheer van het informaticasysteem onontbeerlijk.
Men moet uiteraard rekening houden met de specifieke omstandigheden zoals de gebruikte antivirussoftware.
Op de website van de KSZ vindt u een POLICY die de regels voor het gebruik van een werkpost binnen een sociale zekerheidsinstelling preciseert.

Sommige OCMW's kunnen zich tevens richten tot hun leverancier van sociale software die zich bezighoudt met hun antivirusprogramma of de toegangsleverancier zoals VERA.

Net als voor alle veiligheidsmaatregelen moeten de maatregelen om te beschikken over een gebruikershandleiding met betrekking tot het voorkomen van virusbesmettingen, het gebruik van de antivirussoftware en de te nemen acties in geval van virusinfectie *beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt*.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Norm 4.2.8.2. elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet een geactualiseerde antivirussoftware installeren teneinde virusinfecties te voorkomen, te detecteren en te corrigeren.

Infecties van het informaticasysteem door computervirussen voorkomen, detecteren en corrigeren vormt één van de actuele uitdagingen van elke organisatie. De informatieveiligheidsconsulent van het OCMW waakt er dus over dat een antivirussoftware adequaat wordt geïnstalleerd en zo regelmatig mogelijk bijgewerkt.
De keuze, de installatie en het bijwerken van deze software kan enkel worden verwezenlijkt in nauwe samenwerking met de persoon die is belast met het beheer van het informaticasysteem van het OCMW.
Voor meer informatie, gelieve de helpdesk van de POD MI te contacteren.

Net als voor alle veiligheidsmaatregelen moeten de maatregelen om een geactualiseerde virussoftware te installeren teneinde virusinfecties te voorkomen, te detecteren en te corrigeren beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele verbeteringen die eraan moeten worden aangebracht, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

3.2.9. Toezicht / audit.

Norm 4.2.9. **elk OCMW dat is aangesloten op het netwerk van de Kruispuntbank, moet ten minste één keer om de vier jaar een audit organiseren met betrekking tot de situatie van de logische en fysieke veiligheid.**

De aandachtspunten die tijdens de audit naar boven komen, worden door het OCMW gesignaleerd aan de werkgroep "Informatieveiligheid".

Bovendien zal een samenvatting van de audit overgemaakt worden aan het Toezichtscomité.

Na verloop van 6 maanden moet een evaluatierapport meegedeeld worden aan het Toezichtscomité, waarin een overzicht gegeven wordt van de ondertussen getroffen maatregelen. De originele rapporten zullen beschikbaar moeten blijven voor het Toezichtscomité, zodat het deze kan raadplegen in geval van een incident achteraf.

Het doel van een audit is de werkelijkheid en doeltreffendheid nagaan van de procedures die werden ingesteld om een probleem te voorkomen.
Een audit is een positieve actie om de organisatie te helpen één van de onderdelen van haar veiligheid te evalueren.
Een OCMW dat aangesloten is op het netwerk van de KSZ, is verplicht de nodige maatregelen te nemen of de aanwezigheid ervan na te gaan om de minimale veiligheidsnormen na te leven.
De organisatie van een audit is een gezamenlijke actie van alle betrokken partijen onder leiding van de verantwoordelijke voor het dagelijks bestuur.
Een audit kan worden uitgevoerd door een lid, een team van het OCMW – anders dan de veiligheidsconsulent zelf - een veiligheidsconsulent van een ander OCMW of door een externe organisatie (gemeente, erkende intercommunale, een privé-bedrijf of een erkende gespecialiseerde veiligheidsdienst). Het is belangrijk dat de auditor beschikt over voldoende afstand en kennis van zaken om de te controleren domeinen te evalueren.
Het doel van een audit is vooral gedragslijnen bepalen of voorstellen om waar nodig de zwakke punten te corrigeren. In deze context bestaat de rol van de veiligheidsconsulent, gesteund door de verantwoordelijke voor het dagelijks bestuur, erin de toepassing van de voorgestelde aanbeveling te bevorderen.
In het oorspronkelijke veiligheidsplan zullen enkele pistes worden voorgesteld die het mogelijk maken de prioriteiten binnen de eigen organisatie te identificeren.

Bijvoorbeeld: de audit van de fysieke beveiliging test de goede werking van het inbraaksysteem. Er is in een cascade van 3 telefoonnummers voorzien in geval van inbraak. De audit toont aan dat de eerste aangewezen persoon met vakantie was, de tweede op pensioen is gegaan en de derde van telefoonnummer is veranderd.
De audit zal aanbevelen de procedure bij te werken en minstens één keer per jaar de actualiteit van de procedure na te gaan en ze te testen.

Net als voor alle veiligheidsmaatregelen moet de organisatie, minstens één keer om de vier jaar, van de audit met betrekking tot de situatie van de logische en fysieke veiligheid beantwoorden aan de specifieke behoeften van elk OCMW en dienovereenkomstig worden uitgewerkt.

De eventuele corrigerende maatregelen die te nemen zijn ten gevolge van een audit, kunnen, mits akkoord van de persoon die is belast met het dagelijks bestuur van het OCMW, worden ingeschreven in het veiligheidsplan van het OCMW.

Gegevens van de partners.

POD Maatschappelijke Integratie
G. Kempgens
Veiligheidsconsulent
02.508.86.56
gilles.kempgens@mi-is.be

Helpdesk security POD Maatschappelijke integratie
Helpdesk.security@mi-is.be
02.509.83.48

Administratieve cel
Dhr. M. Goffin
02.509.59.71
marcel.goffin@smals-mvm.be

Erkende Gespecialiseerde Veiligheidsdienst
Dhr. J. Costrop
02.509.57.55
johan.costrop@smals-mvm.be

Veiligheidsdienst Kruispuntbank van de Sociale Zekerheid
Dhr. Jean-Marie Gossiaux
Veiligheidsconsulent
02.741.83.30
jean.marie.gossiaux@bcss.fgov.be

Dienst « Projectbeheer » van de Kruispuntbank van de Sociale Zekerheid (OCMW)
Dhr. Mark Stockx
02.741.84.85
mark.stockx@ksz.fgov.be

Helpdesk van de Kruispuntbank van de Sociale Zekerheid
02.741.83.11
helpdesk.security@mi-is.be

VVSG
Chris Boens
Chris.boens@VVSG.be
http://www.vvsg.be/nl/werking_organisatie/ict_en_e-government/kruispuntbank_sociale_zekerheid.shtml

AVCB
Christian Lejour
Christian.lejour@avcb-vsgb.be

UVCW
Sébastien Lemaître
sebastien.lemaitre@uvcw.be

V-ICT-OR
security@v-ict-or.be

Veiligheidskit
GIDS VOOR DE TOEPASSING VAN DE MINIMUMNORMEN