Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
Norm 4.1 Iedere instelling van sociale zekerheid aangesloten op het netwerk van de Kruispuntbank moet een permanent bijgewerkt formeel beleid voor informatiebeveiliging hebben *Uitvoeringsdatum: 01/07/2001*.	Beveiligingsbeleid	Veiligheidsadviseur	-	1 dag	**Actieplan** Het formeel beveiligingsbeleid aangereikt door de KSZ overnemen en het aanpassen aan de interne behoeften van het OCMW. Het door het Permanent Bureau aangepast beveiligingsbeleid voorstellen en laten goedkeuren. **Planning.** Voorlegging aan het Permanent Bureau tijdens het eerste kwartaal en opvolging tijdens het tweede kwartaal.
Norm 4.2 **4.2. Organisatie van de beveiliging**	Organisatorische				
4.2.1. Iedere instelling van sociale zekerheid aangesloten op het netwerk van de Kruispuntbank moet:					
4.2.1.1. een dienst informatiebeveiliging intern organiseren, die onder leiding staat van een adviseur informatieveiligheid, of deze taak toevertrouwen aan een gespecialiseerde dienst voor informatiebeveiliging		Secretaris / Voorzitter / Permanent Bureau	1 dag/week	1 dag/week	**Actieplan** Een veiligheidsadviseur door het Permanent Bureau laten benoemen. Voorlegging aan het Permanent Bureau tijdens het eerste kwartaal en opvolging tijdens het tweede kwartaal.
4.2.1.2. de identiteit van zijn veiligheidsadviseur en van zijn eventuele adjuncten mededelen aan de veiligheidsadviseur van de POD MI.		Veiligheidsadviseur	-	1 uur	De officiële beslissing van het Permanent Bureau verzenden naar de POD MI.
4.2.1.3. beschikken over een veiligheidsplan goedgekeurd door de verantwoordelijke instantie van de betrokken instelling.		Veiligheidsadviseur	1 dag	1 dag	Op basis van de inventaris van de vastgestelde zwakke punten ten opzichte van de minimumnormen, een actieplan opmaken om deze zwakke punten op 3 jaar tijd of meer weg te werken.

Met opmerkingen [hsc1]: [100]
BCSS
==>
KSZ

Met opmerkingen [hsc2]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.2.1.4. beschikken over de nodige werkingskredieten die door de verantwoordelijke instantie van de betrokken instelling zijn goedgekeurd en die ingeschreven zijn in een apart vastgelegd veiligheidsbudget, om haar veiligheidsplan te kunnen uitvoeren		Permanent Bureau		- 30’	De in het veiligheidsplan voorziene uitgaven door het Permanent Bureau laten goedkeuren. Met de goedkeuring van de secretaris (secretaresse), de ontvanger vragen de uitgaven inzake informaticabeveiliging in een aparte begrotingspost in te schrijven.
4.2.1.5. de POD MI het aantal uren mededelen, die het OCMW officieel heeft toegewezen aan zijn veiligheidsadviseur en aan zijn eventuele adjuncten om hun taken te kunnen uitvoeren (4) .		Veiligheidsadviseur	-	1 uur	Het officieel document van het Permanent Bureau waarin het aantal officieel toegewezen uren is vermeld naar de POD MI verzenden.
4.2.1.7. beschikken over procedures voor de mededeling van informatie aan de veiligheidsadviseur, zodat laatstgenoemde in het bezit is van de gegevens waardoor hij de hem toevertrouwde opdracht kan vervullen.		Secretaris en veiligheidsadviseur en iedere andere betrokken persoon	-	Te ramen	Het verzamelen van informatie organiseren door middel van een periodieke veiligheidsvergadering met de betrokken dienstchefs. Een procedure uitwerken met de dienst Personeel voor de aankomende en vertrekkende personeelsleden, om problemen in verband met de toegang tot het netwerk op te lossen. Invoering van een systeem voor het verlenen, het afschaffen en het intrekken van toegang op basis van een schriftelijke of informaticaprocedure die kan worden teruggevonden. Eenvoudige procedures invoeren om de andere diensten te betrekken en alle informatie die een weerslag heeft op beveiliging te verzamelen (panne van server, panne van klimaatregeling, panne van het systeem voor toegangscontrole, incidenten, …). Eventueel, een incidentenregister opmaken, die voor iedereen toegankelijk is.

Met opmerkingen [hsc3]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.2.1.8. beschikken over procedures voor het organiseren van het overleg tussen de verschillende partijen (6) om de veiligheidsadviseurs nauwer te betrekken bij de werkzaamheden van de instelling			Te ramen	Te bepalen	Idem
4.3. Fysische beveiliging en beveiliging van de omgeving	Fysische beveiliging				
Iedere instelling van sociale zekerheid aangesloten op het netwerk van de Kruispuntbank moet:					
4.3.1. de toegang tot de gebouwen en lokalen beperken tot de gemachtigde personen en deze toegang controleren zowel tijdens als buiten de diensturen.		Veiligheidsadviseur, secretaris en IDPBW-verantwoordelijke	Te ramen	Te bepalen	Zorgen voor de beveiliging van de fysische toegangen tot het OCMW naar gelang van de risico's die de omgeving inhoudt. Ervoor zorgen dat niemand het OCMW kan betreden zonder zich te moeten aanmelden. Indien de indeling van het gebouw het toelaat, is het niet nodig een systeem voor geautomatiseerde toegangscontrole te installeren. Ervoor zorgen dat niemand in het OCMW kan rondlopen zonder door iemand te worden vergezeld.

Met opmerkingen [hsc4]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc5]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.3.2. maatregelen treffen inzake preventie, bescherming, detectie, blussen en interventie op het gebied van brand, inbraak en waterschade.		Veiligheidsadviseur, secretaris en IDPBW-verantwoordelijke	Te ramen naar gelang van de behoeften	1 dag per maand of meer naar gelang van de behoeften	Een of meerdere ontruimingsploegen organiseren en ieder jaar een ontruimingsoefening houden. Het eerste jaar laten weten op welke dag de oefening plaatsheeft en het tweede jaar tijdens welke week de oefening plaatsheeft. Een balans opmaken van de ontruiming na de oefening en de zwakke punten wegwerken aan de hand van een lijst van de acties die tijdens de ontruiming moeten worden ondernomen (sluiten van de deuren, controleren dat niemand achterblijft, enz.). Indien nodig een interventieploeg organiseren en een behoorlijke basisopleiding voorzien bij de brandweer van de gemeente of bij een gespecialiseerde instelling of firma. Een inventaris opmaken van de risico's verbonden aan brand, waterschade en gas. De beveiliging van de lokalen controleren (inbraakalarm, codesloten, enz.), de lokalen met kostbaar materieel afschermen (gordijnen, stores), de inventaris opmaken van de bestaande of te nemen maatregelen (te installeren brandblusser, deur met een stang voor automatische ontgrendeling, …). Een beroep doen op de IDPBW-verentwoordelijke, de brandweer, de politie of de gespecialiseerde firma om de risico's te verminderen. Telkens verschillende oplossingen onderzoeken, het noodzakelijk investeren in al dan niet automatische beveiliging evalueren. Bijzondere aandacht besteden aan de klimaatregeling en aan de onderhoudscontracten.

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.3.2. maatregelen treffen inzake preventie, bescherming, detectie, blussen en interventie op het gebied van brand, inbraak en waterschade (vervolg)					Het bestaan van een contract voor bijstand en vervanging van het informaticamaterieel in geval van technische panne of beschadiging nagaan en evalueren of dergelijk contract noodzakelijk is. Ook de dekking door de verzekeringen nagaan.
4.3.3. beschikken over een alternatieve elektrische voeding om de informaticaoperaties zonder risico's te kunnen afsluiten (wanneer ze gegevens in het kader van de sociale zekerheid verstrekken).		Veiligheidsadviseur en informatica-verantwoordelijke	1/2 dag	1/2 dag	Deze elektrische voeding kan: - voor de grotere OCMW's een dieselmotor, een batterijsysteem, een alternatieve voeding, een UPS beperkt tot een batterij, enz. zijn; - voor de OCMW's met een kleine informatica-uitrusting, een UPS met batterij zijn, waarvan het programma op de server is geïnstalleerd en waardoor de lopende operaties kunnen worden beëindigd zonder gegevensverlies Het is belangrijk na te gaan dat de batterijen (en de andere systemen) gebruiksklaar zijn en dat een werkingstest wordt georganiseerd op basis van een simulatie.
4.4. Logische beveiliging van de toegang	Informaticabeveiliging				
4.4.1. de toegang tot de gegevens (7) die nodig zijn voor de applicatie en voor de uitvoering van de sociale zekerheid beveiligen door middel van een identificatie-, authentificatie- en machtigingssysteem.		Veiligheidsadviseur en informatica-verantwoordelijke	Te ramen op basis van de behoeften	Idem	Een gebruikersnaam voor iedere gebruiker creëren en hem een paswoord van 8 tekens of symbolen opleggen, dat om de drie maanden moet veranderd worden. De gebruiker moet zijn paswoord alleen kunnen kiezen, dat noch de veiligheidsadviseur noch de informaticus mogen kennen. Voor dringende gevallen, het paswoord onder gesloten en ondertekende omslag ter beschikking stellen van de netwerkbeheerder en van zijn adjunct of van de aangewezen persoon in geval van afwezigheid.

Met opmerkingen [hsc6]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc7]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.4.2. een loggingsysteem implementeren voor de persoonsgegevens die nodig zijn voor de applicatie en voor de uitvoering van de sociale zekerheid.		Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	Te ramen	Idem	De loggingsystemen moeten het mogelijk maken te weten wie wat heeft gedaan en vooral: 1. op het niveau van de aansluitingen op het netwerk van de sociale zekerheid door de gebruikers; 2. in de applicaties gebruikt door de maatschappelijk en administratief assistenten; 3. in iedere applicatie met uitwisseling van gegevens met het extranet van de sociale zekerheid (KSZ-netwerk) en in elke gevoelige applicatie met gegevens van sociale aard. Deze loggings omvatten ook de bewaring van de gegevens : wijze van bewaring (op welke drager), duur, beveiliging, doel, enz.
4.4.3. een systeem van veiligheidskopie (back-up) invoeren, dat regelmatig wordt gecontroleerd, waardoor men ervoor kan zorgen dat in geval van totaal of gedeeltelijk ernstig defect de gegevens niet onherstelbaar verloren zijn gegaan (gegevens nodig voor de applicatie en voor de uitvoering van de sociale zekerheid en gegevens betreffende de applicaties en het exploitatiesysteem)		Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	2 dagen	Idem	Het invoeren van back-upsystemen moet aan meerdere eisen voldoen: - zorgen voor het saven van de gebruikte gegevens en dit voor de nodige duur voor het goed heropstarten van de activiteiten van het OCMW, bijvoorbeeld: de bewaringsduur van de back-ups moet het voor het OCMW mogelijk maken om de uitbetalingen te doen (eventueel op basis van de laatste verrichte betalingen) ; - zorgen voor het saven van de exploitatiesystemen om alles opnieuw te kunnen installeren in geval van ernstig defect; - beschikken over een systeem waarbij het behoorlijk saven van de back-ups kan worden gecontroleerd om de informaticadragers tijdig te kunnen vervangen; - zorgen voor het saven op een plaats buiten het OCMW.

Met opmerkingen [hsc8]: [100]
BCSS
==>
KSZ

Met opmerkingen [hsc9]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc10]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc11]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.4.4. een systeem evenals formele en bijgewerkte procedures invoeren, waardoor overtredingen inzake veiligheid kunnen worden opgespoord, opgevolgd en rechtgezet.		Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	Een IDS kost minimum 2.000 € zonder het geschikte personeel.	Voor een IDS is de aanwezigheid van een persoon iedere dag voltijds achter het controle-scherm nodig.	Tenzij een IDS wordt geïnstalleerd, dat enkel kan worden gebruikt door OCMW's met aanzienlijke middelen, beantwoordt enkel een louter administratieve procedure op basis van de officiële mededeling van anomalieën vastgesteld door de gebruikers aan deze norm. De anomalieën kunnen ook vastgesteld worden door de veiligheidsadviseur door de logs van de beschikbare auditsystemen te controleren vanuit een XP pro of gelijk welke omgeving met systemen voor audit en geïntegreerde beveiliging.
4.4.5. Wanneer de instelling, in de zone « USERID » van het prefixdeel van het bericht dat ze naar de Kruispuntbank zendt, het nummer vermeldt van het programma dat het bericht voor de Kruispuntbank heeft gecreëerd, alhoewel dit bericht van een fysische persoon uitgaat, kan de Kruispuntbank het nummer van dit programma achteraf terugvinden. De Kruispuntbank kent evenwel niet de identiteit van de fysische persoon die dit bericht heeft verzonden. In dit geval moet de sociale instelling dus de koppeling maken tussen het nummer van het programma dat ze vermeldt in het prefixdeel van het bericht, dat ze naar de Kruispuntbank zendt, en de identiteit van de fysische persoon die het bericht creëert.		Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	½ dag	½ dag	Procedure te bepalen en inventaris op te maken met de informaticafirma die de sociale applicatie levert, indien het OCMW op haar een beroep doet, en met de verantwoordelijke informaticus. Een procedure moet worden bepaald voor de toekenning en de afschaffing van gebruikersnamen of –nummers en van paswoorden en voor de inventaris van de identiteiten van de gebruikers aangezien hun toegangen daarin vermeld moeten zijn. Deze inventaris moet constant worden bijgewerkt. De diensten informatica,veiligheid en personeel zijn bij deze procedure betrokken.

Met opmerkingen [hsc13]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc12]: [100]
adéquat
==>
afdoend

Met opmerkingen [hsc14]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.5. Ontwikkeling, productie en onderhoud van de applicaties Iedere instelling van sociale zekerheid aangesloten op het netwerk van de Kruispuntbank moet:					
4.5.1. beschikken over formele en bijgewerkte procedures voor het in productie stellen van nieuwe applicaties en het aanbrengen van aanpassingen in de bestaande applicaties om te voorkomen dat een en dezelfde persoon dit proces zou controleren.		Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	Te evalueren	Te evalueren	Wat betreft de OCMW's die een beroep doen op leveranciers van informatica-applicaties, zijn de leveranciers verantwoordelijk voor deze norm. Voor de andere OCMW's die over een voldoend gestructureerd informaticateam beschikken, is deze norm van toepassing.
4.5.2. beschikken over formele en bijgewerkte procedures voor het opmaken van de documentatie bij de ontwikkeling van nieuwe applicaties en systemen en bij het onderhoud van de bestaande applicaties en systemen (8).		Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	5 dagen	5 dagen	Het bijwerken van de documentatie is belangrijk. Voor OCMW's die werken met leveranciers van gelijk welke applicaties, is het van belang dat ze in hun contract het saven van hun applicaties voorzien (broncodes) bij een vertrouwenspersoon (notaris, deurwaarder, overheid, enz.) en de documentatie in geval van faillissement van de leverancier. Voorzichtigheidshalve moet de versie en de documentatie bij de vertrouwenspersoon regelmatig worden bijgewerkt.

Met opmerkingen [hsc15]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc16]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc17]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.6 Beveiliging van het netwerk Ieder OCMW aangesloten op het netwerk van de Kruispuntbank moet :					
4.6.1. de toegang tot het informaticasysteem (de informaticasystemen) beperken tot de geïdentificeerde, geauthentificeerde en gemachtigden personen/voorwerpen.	Fysische en informaticabeveiliging	Veiligheidsadviseur, informatica-verantwoordelijke / dienst gespecialiseerd in informatie-beveiliging	Naar gelang van de kosten van de te voorziene beveiliging	Naar gelang van het aantal gebruikers en de gebruikte omgeving	Alle systemen voor het beheer van het informaticanetwerk installeren in daartoe voorziene lokalen, de toegangen tot de informaticasystemen (servers, modems, routers, switches, enz.) beperken tot enkel de betrokken personen (de systeembeheerder, de netwerkverantwoordelijke, de leverancier).
4.6.2. een systeem evenals formele en bijgewerkte procedures invoeren, waardoor overtredingen inzake veiligheid kunnen worden opgespoord, opgevolgd en rechtgezet.	Informaticabeveiliging	Adviseur informaticaveiligheid, informatica-verantwoordelijke, leverancier sociale applicatie	Een IDS kost minimum 2.000 € zonder het geschikte personeel.		Tenzij een IDS wordt geïnstalleerd, dat enkel kan worden gebruikt door de bezitters van omvangrijke systemen, beantwoordt enkel een louter administratieve procedure op basis van de officiële mededeling van anomalieën vastgesteld door de gebruikers aan deze norm. De anomalieën kunnen ook vastgesteld worden door de veiligheidsadviseur door de logs van de beschikbare auditsystemen te controleren vanuit Windows 2000 of gelijk welke omgeving met systemen voor audit en geïntegreerde beveiliging zoals de netwerkmonitor.
4.6.3. De OCMW's kunnen het Extranet van de sociale zekerheid gebruiken voor de TCP/IP verbindingen buiten de sociale zekerheid. Voor hun rechtstreekse verbindingen met de TCP/IP netwerken buiten de sociale zekerheid moeten de OCMW's veiligheidsmaatregelen toepassen die in overeenstemming blijven met de maatregelen die op het niveau van het Extranet van de sociale zekerheid worden getroffen.	Informaticabeveiliging	Veiligheidsadviseur, informatica-verantwoordelijke			Goed om weten is dat een perfect beveiligd intern netwerk slechts doeltreffend is wanneer al zijn ingangen worden gecontroleerd. Men moet er dan ook voor zorgen dat alle aansluitingen naar buiten voldoen aan dezelfde veiligheidsregels, namelijk ten minste aan de minimumnormen.

Met opmerkingen [hsc18]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc20]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc19]: [100]
adéquat
==>
afdoend

Met opmerkingen [hsc21]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc22]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.7. Continuïteitsplan Ieder OCMW aangesloten op het netwerk van de Kruispuntbank moet :					
4.7.1. een risico-onderzoek uitvoeren om een continuïteitsplan te kunnen opmaken.	Organisatorische	Veiligheidsadviseur		Naar gelang van de grootte van het OCMW en van de hoeveelheid risico's, van meerdere uren tot meerdere dagen	Ieder veiligheidsaspect uiteengezet in het deel over de minimale veiligheidsvoorwaarden overlopen en inschatten welke problemen het OCMW in de praktijk zou tegenkomen in geval van zeer ernstig defect. Men moet dan de waarschijnlijkheid dat het incident zich zou kunnen voordoen en de weerslag ervan op het beheer van de instelling evalueren: een verhoogd risico verdient bijzondere aandacht.
4.7.2. een continuïteitsplan opmaken, uittesten en in stand houden om de opdrachten van het OCMW op het gebied van sociale zekerheid te kunnen garanderen. Daarin moet daarenboven een plaats voor informaticamigratie voorzien zijn in geval van gedeeltelijk of geheel ernstig defect.	Organisatorische	Veiligheidsadviseur, informatica-verantwoordelijke en iedere betrokken persoon			Naar gelang van de punten vermeld in de risicoanalyse, beschrijft de veiligheidsadviseur in het continuïteitsplan alle acties die moeten worden ondernomen bij een incident. Het is van belang dat iedere persoon die moet optreden op de hoogte is van de bepalingen van het continuïteitsplan opdat, zelfs wanneer de veiligheidsadviseur afwezig is, maatregelen kunnen worden getroffen om het OCMW opnieuw op te starten binnen de door het centrum voorziene termijn.
4.8. Inventaris Ieder OCMW aangesloten op het netwerk van de Kruispuntbank moet :					
4.8.1 beschikken over een voordturend bijgewerkte inventaris van het informaticamaterieel en van de programmatuur	Fysische beveiliging	Veiligheidsadviseur	Naar gelang van het aantal gebruikers	Een uur tot meerdere uren (soms dagen voor de grotere OCMW's).	Deze inventaris heeft tot doel een volledige lijst op te maken van de programma's, het materieel, de netwerken, … die worden gebruikt om, in een geval van zeer ernstig defect, de meest volledige en meest passende werkomgeving naar gelang van de prioriteiten te herstellen.

Met opmerkingen [hsc23]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc25]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc24]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc26]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc27]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc28]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc29]: [100]
permanence
==>
zitdag

Met opmerkingen [hsc30]: [100]
CPAS
==>
OCMW

Minimumnorm	Soort beveiliging	Verantwoordelijke	Geraamde kost	Werklast	Te ondernemen acties / stand van zaken
4.9. Beveiliging tegen infecties door informaticavirussen					
4.9.1. beschikken over een gebruikshandleiding over het voorkomen van infecties door virussen, over de werking van de geïnstalleerde antivirusprogrammatuur en over de acties die moeten worden ondernomen in geval van infectie door een virus.	Informaticabeveiliging	Informatica-verantwoordelijke en de dienst informatica	Nihil	Nihil	De handleiding wordt samen met de programmatuur geleverd. Ze moet voorzichtigheidshalve worden gelezen en het nodige moet worden gedaan (heropstartdiskette) om te kunnen optreden in geval een virus in een PC of in het netwerk aanwezig is.
4.9.2. een bijgewerkte antivirusprogrammatuur installeren om infecties door informaticavirussen te voorkomen, op te sporen en te behandelen.	Informaticabeveiliging	Informatica-verantwoordelijke en de dienst informatica	Naar gelang van het aantal gebruikers	Een uur tot meerdere uren (soms dagen voor de grotere OCMW's).	Het louter installeren van het antivirusprogramma is geen oplossing op zichzelf; dit programma moet nog bijgewerkt worden, onder andere door de nieuwe ontdekte virussen te melden opdat het programma ze zou kunnen opsporen. Dit wordt het bijhouden van de lijst van de « signaturen » van virussen genoemd. Dit moet zo vaak mogelijk gebeuren (idealiter alle dagen) en ten minste een keer bij elke belangrijke waarschuwing (door de media of de antivirussites bijvoorbeeld).
4.10. Toezicht / audit					
Ieder OCMW aangesloten op het netwerk van de Kruispuntbank moet :					
ten minste een keer om de vier jaar een audit organiseren over de situatie van de beveiliging zowel op logisch als op fysisch niveau.	Beleid voor het controleren van de beveiliging	Alle diensten betrokken bij informatiebeveiliging	Veranderlijke kost naar gelang van de aard van de audit (fysische audit en informatica-audit)	Een dag tot meerdere dagen naar gelang van de omvang van de installaties	Door het ondervragen van de actoren en door middel van toetsingen heeft het audit tot doel de aandacht te vestigen op de fundamentele logische en fysische zwakken punten bij een bepaald OCMW . De kosten kunnen worden beperkt door een andere veiligheidsadviseur bij een OCMW een interne audit in het eigen OCMW te laten verrichten.

Met opmerkingen [hsc31]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc32]: [86]
instaatstelling
==>
mise en état

Met opmerkingen [hsc33]: [100]
CPAS
==>
OCMW

Met opmerkingen [hsc34]: [100]
CPAS
==>
OCMW