Toelichting bij de minimale veiligheidsnormen

Bavo Van den Heuvel
Veiligheidscel POD Maatschappelijke Integratie

12 januari 2005 v1.4

POD Maatschappelijke Integratie
SPP Intégration Sociale

Programma van de dag

- 9h-12h: deel 1 rond de minimale veiligheidsnormen
- 12h-13h: middagpauze
- 13h-15h: deel 2 rond de minimale veiligheidsnormen
- 15h-16h: beveiligingsaudit ter plaatse bij het OCMW om de theorie aan de praktijk te koppelen

Veiligheidscel: OCMW's helpen in hun aansluiting naar de Kruispuntbank van de Sociale Zekerheid op het vlak van veiligheid

Voor vragen over de stromen en de KSZ:

- VVSG: chris.boens@vvsg.be of anne-marie.engelen@vvsg.be
- KSZ:
  - **Tel : 02/509 58 27**
  - **E-mail : OCMW-CPAS@SmalS-MvM.be**

- Deze cel heeft als missie:
  - **het organiseren van het veiligheidsbeleid van de POD MI**
  - **het organiseren van veiligheidsacties ten bate van de 589 OCMW's**
- Doel van de helpdesk: het helpen en informeren van de veiligheidsconsulenten
- E-mail: helpdesk.security@mi-is.be
- Tel: 02/509.83.48 (elke dinsdag)

Doel van deze opleiding

- Doel opleiding: minimale veiligheidsnormen vertalen naar OCMW-wereld
- Gevorderde OCMW's
- Beginnende OCMW's

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Vragen na opleiding

- Graag hadden we van elk OCMW een top-5 van vragen gekregen
- Sturen naar helpdesk.security@mi-is
- Basis voor FAQ
- Herinneringsmail
- Stel vragen nu

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Iets over de risico's waartegen beschermd wordt:
1 Vertrouwelijkheid

- Definitie: **Vertrouwelijkheid** is de mate waarin de bevoegdheid en de **mogelijkheid** tot lezen, kopiëren of kennisnemen wordt **beperkt tot een gedefinieerde groep van gerechtigden**.

Schending van vertrouwelijkheid

Voorbeelden misbruik gegevens die men via de KSZ opvraagt:

- **Verzekeringen**
- **Een relatiebureau**
- **Een bedrijf in kindervoeding**

Commerciële belangen vs juiste gegevens.

Andere voorbeelden.

Iets over de risico's waartegen beschermd wordt: 2 Integriteit

- Definitie: Integriteit staat voor de correctheid en volledigheid van informatie en de verwerking.
- Praktisch: elektronisch eenvoudig, op papier moeilijker
- Opzettelijke of abusievelijke fouten:
  - **Opzettelijke fouten zijn bijvoorbeeld manipulatie van invoerdocumenten, programma's en verwerkingen en het ongeautoriseerd wijzigen van bestanden.**
  - **Abusievelijke fouten zijn bijvoorbeeld programmafouten, storingen en foute gegevensinvoer.**
- Voorbeelden

Schending van integriteit

Als er geen integriteit is ….,

na een inbraak thuis is de integriteit van je privé-bezit aangetast

Iets over de risico's waartegen beschermd wordt: 3 Beschikbaarheid

- **Definitie: Beschikbaarheid:** kunnen we als geauthoriseerde gebruiker tijdig over de gegevens beschikken die we nodig hebben voor de uitvoering van onze taken.

5040D mediabox
tbv digitale informatiedragers
kbr6205810

5040D mediabox, t.b.v. brandwerende opberging van digitale informatiedragers (zoals CD-R, diskettes, datatapes e.d.). Buitenmaat 32.5x40x31.8cm, binnenmaat 22x13x15cm. Deze mediabox heeft de tetst van 1 uur in de volle brand voor digitale informatiedragers goed doorstaan. Bij een omgevingstemperatuur van ongeveer 1000°C blijft de binnentemperatuur beneden het kritieke punt van 52°C. Kan zeer goed in combinatie met brand- en braakwerende archiefkast worden gebruikt.

€ 259.86

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Gebrek aan beschikbaarheid

- Als er geen beschikbaarheid is, kan het OCMW niet verder werken met alle menselijke en politieke drama's die daarbij horen.
- Tegenstrijdigheid tussen vertrouwelijkheid en beschikbaarheid

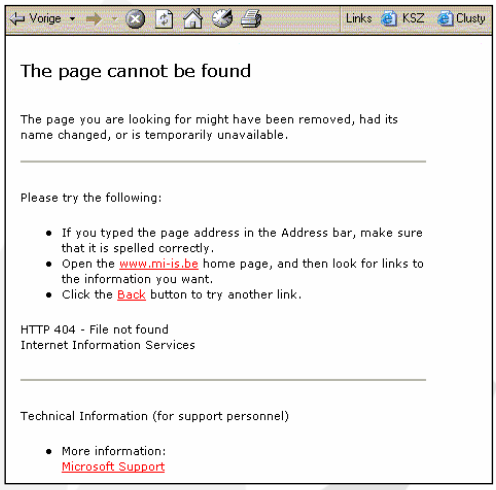
Banksys-betaalsysteem weigert dienst bij 127.000 aankopen

Afgelopen zaterdagmiddag, uitgerekend tijdens een van de belangrijkste verkoopweekends van het jaar, lieten de betaalautomaten van Banksys het bij 127.000 transacties afweten. Het ging om 100.000 betalingen via Bancontact/Mister Cash en 27.000 betalingen met kredietkaarten Visa en Mastercard. Banksys had gisteren nog geen uitleg voor de onverwachte panne, maar het vermoeden luidt dat het centrale computersysteem het probleem veroorzaakte.

Banksys reageert met de melding dat de pannes slechts iets meer dan 3 procent van de debettransacties vertegenwoordigden, en iets meer dan een kwart van de kredietkaartbetalingen, maar de handelaars en warenhuizen die werden getroffen door de pannes waren er niet blij mee. Retailers schatten de schade op enkele miljoenen euro, de distributeursfederatie Fedis denkt zelfs aan een omzetverlies van 20 procent. Zelfstandigenorganisatie Unizo denkt zelfs een vergoeding te eisen aan Banksys. Ze gaat daarvoor vandaag rond de tafel zitten met de operator. "Honderdzevenentwintigduizend gemiste transacties is veel, laat daar geen twijfel over bestaan", zegt distributiehoofd Luc Ardies van Unizo. "Bovendien zegt het cijfer niet alles over het probleem en de geleden schade: de panne veroorzaakte ook een chaos op een erg druk moment, er zijn consumenten die hun winkelkarretje of hun waren noodgedwongen moesten laten staan."

(RMe)

Algemeen, pagina 3

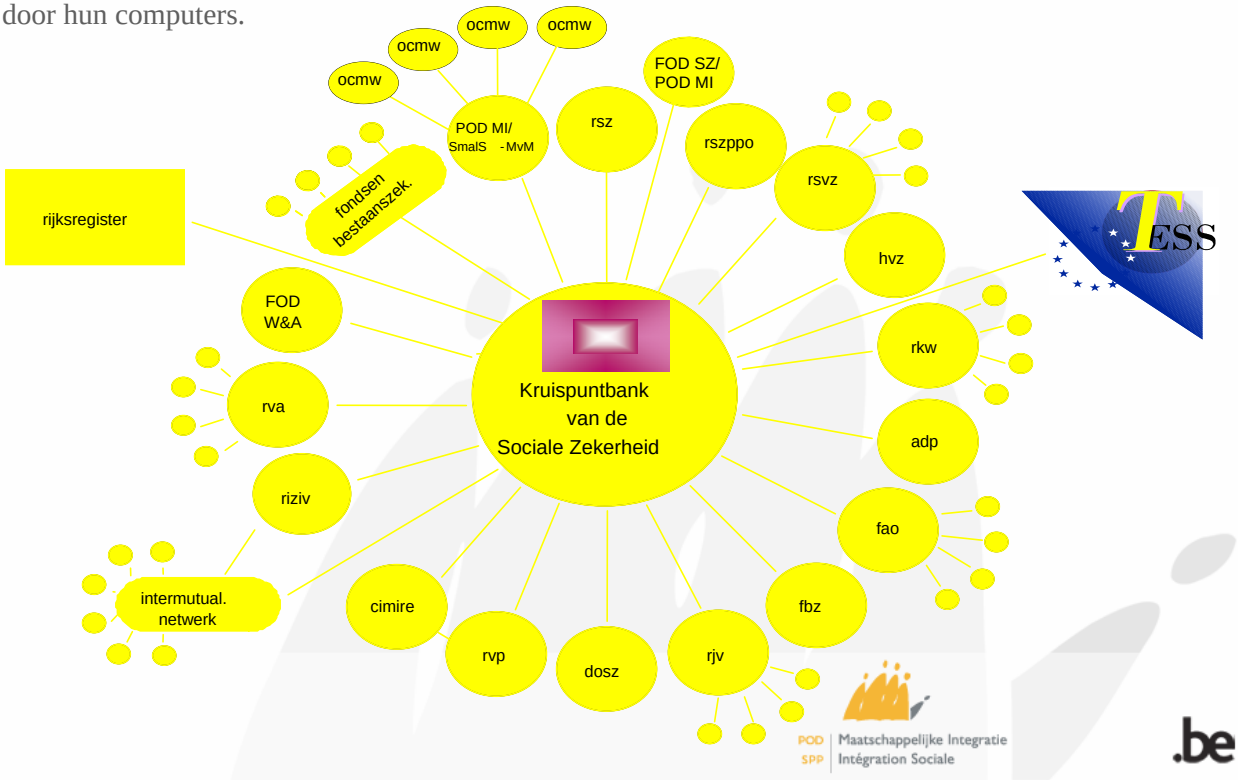


POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Kruispuntbank

- De kruispuntbank is een elektronisch netwerk tussen de instellingen van de sociale zekerheid en het rijksregister. De verschillende instellingen zijn met elkaar verbonden door hun computers.



De berichten voor de OCMW's

- Consultatie van het Rijks-, BIS- en Kruispuntbankregister, Wachtregister voor asielzoekers
- Integratie leefloondossier in repertoria van KSZ en POD MI (SmalS-MvM)
- Wijziging van een integratielijn in de repertoria
- Consultatie van het secundair repertorium van de POD MI: info van andere OCMW's
- Consultatie van het personenrepertorium van de Kruispuntbank: waar is persoon gekend?

De berichten voor de OCMW's

- Multifunctioneel attest afkomstig van de OCMW's bestemd voor de verzekeringsinstellingen en de kinderbijslagsector
- Loopbaanattest zelfstandigensector
- Consultatie van de verzekerbaarheidssituatie bij de verzekeringsinstellingen
- Aangifte leefloon aan POD MI (A053)

Minimale veiligheidsnormen

Bron: http://www.bcss.fgov.be/documentation/nl/s%E9curit%E9/v2002.253.normen.pdf

2.1 Toepassingsgebied van de normen:

- De implementatie en de verificatie van de minimale veiligheidsnormen bij derden, die .. sociale gegevens van persoonlijke aard verwerken, behoren in eerste instantie tot de verantwoordelijkheid van het OCMW die aan de derde werkzaamheden toevertrouwde.

Minimale veiligheidsnormen

- Op basis van de vragenlijsten die door de OCMW's teruggestuurd worden, kan de POD MI in deze OCMW's, na een aankondiging, controles laten uitvoeren door een externe instantie met betrekking tot de naleving van specifieke aspecten van de minimale veiligheidsnormen.
- Verder zijn de normen enkel van kracht op de verwerking van sociale persoonsgegevens.

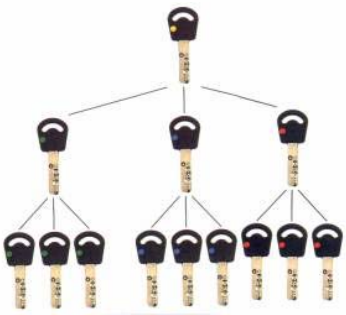
POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Minimale Veiligheidsnormen

2.2. Interpretatie van de normen

- De sociale instellingen dragen de verantwoordelijkheid om, in functie van hun specifieke situatie en al naargelang de belangrijkheid van de te beveiligen werkingsmiddelen, de meest aangewezen beveiligingsmaatregelen te implementeren.



POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.1 "Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet over een formeel en permanent bijgestuurd informatieveiligheidsbeleid beschikken"

Informatiebeveiliging:
voorkomen en herstellen van schade aan sociale gegevens en van onrechtmatige schendingen van de persoonlijke levenssfeer van de betrokkenen.

(Art 1 KB120893 Informatieveiligheid)

Bron: http://www.bcss.fgov.be/documentation/nl/s%E9curit%E9/v2002.253.normen.pdf

Doel informatieveiligheidsbeleid:

- **sensibilisering** omtrent de risiko's
- **opzetten van een organisatie**
- het **bevorderen van de coördinatie en de uitvoering** van de veiligheidsmaatregelen
- het **niveau van vertrouwen in informatica** binnen de instelling **verhogen**.

4.2.1.1 Veiligheidsconsulent

- De veiligheidsconsulent is er om het OCMW te helpen
- Taken
- **De verantwoordelijkheid** van de veiligheidsconsulent

Zie ook **12 AUGUSTUS 1993. - Koninklijk besluit houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid** Hoofdstuk II (een OCMW is in deze zin een instelling van sociale zekerheid)

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Jaarlijks verslag

KB 120893 Art. 8. jaarverslag omvat **minstens** :

1° een algemeen overzicht van de veiligheidstoestand, de evolutie in het afgelopen jaar en de nog te realiseren doelstellingen;

2° een samenvatting van de schriftelijke adviezen en het gevolg

3° een overzicht van de werkzaamheden

4° een overzicht van de resultaten van de controles

5° (...)

6° (...)

7° een overzicht van de gevoerde campagnes

8° een overzicht van alle gevolgde en de voorziene nog te volgen opleidingen.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.2 Identiteit meedelen

4.2.1.2. “de **identiteit van haar veiligheidsconsulent** en haar eventuele adjuncten **meedelen** aan het Toezichtscomité bij de Kruispuntbank van de Sociale Zekerheid (thans sectoraal comité van de sociale zekerheid).”

- Opsturen aan: POD MI, tav Gilles Kempgens, Anspachlaan 1, 1000 Brussel.
- Tevens aantal toegekende uren
- Goedgekeurd door OCMW

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.3 Goedgekeurd veiligheidsplan en werkkredieten

4.2.1.3. “in het bezit zijn van een **veiligheidsplan** dat door de verantwoordelijke instantie van de betrokken instelling werd **goedgekeurd**.”

Men dient “in het bezit te zijn” van een goedgekeurd veiligheidsplan.

Een veiligheidsplan is een plan dat uit verschillende delen wordt opgemaakt:

- evolutie verleden jaar
- plannen van het OCMW binnen de 3 volgende jaren
- schatting van de kosten en de nodige tijd voor de realisatie van de acties insluiten

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.4 Werkkredieten hebben

- over de nodige **werkkredieten** beschikken
- **goedgekeurd**
- in een afzonderlijk gedefinieerd **veiligheidsbudget**
- **teneinde te kunnen voorzien in de uitvoering van haar veiligheidsplan**

4.2.1.5 Uren veiligheidsconsulent

4.2.1.5. aan de POD MI het **aantal uren meedelen dat ze officieel aan de veiligheidsconsulent** en aan zijn eventuele adjuncten **hebben toegekend voor de uitvoering van hun taken** "

- Indicatie van hoeveel werk er kan verricht worden
- Officieel op papier
- Combineren met andere taken

4.2.1.6 Beroepskaart geneeskundige verzorging

4.2.1.6. “de betrokken **veiligheidsconsulenten waken**, binnen de eigen instelling, **over het veilige gebruik van de beroepskaart voor een geneeskundige verzorging** zoals vastgelegd in de artikels 42 tot en met 50 van het koninklijk besluit van 22 februari 1998 “

- Inventaris: SIS en SAM kaarten en lezers
- Wordt verwijderbare kaart onbewaakt achtergelaten?
- Wordt beroepskaart op veilige plaats bewaard?

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

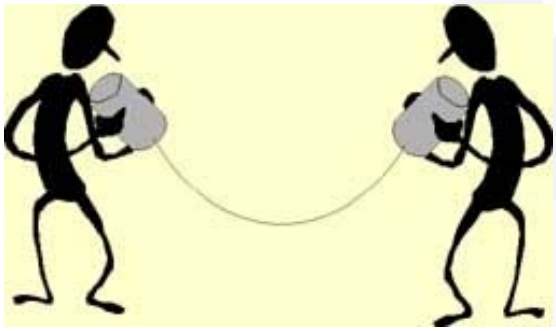
4.2.1.7 Communicatie naar veiligheidsconsulent

4.2.1.7. “**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.”

- actuele en juiste gegevens voor de veiligheidsconsulent
- wat doorgeven?

Communicatiekanaal:

- **niet gevoelige informatie:** e-mail en fax
- geen e-mail of fax voor “**gevoelige informatie**”



POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.2.1.8 Overleg betrokken partijen

4.2.1.8. “over **procedures beschikken met als doelstelling om overleg te organiseren tussen de verschillende betrokken partijen** teneinde op deze manier de veiligheidsconsulenten nauwer te betrekken bij de werkzaamheden van de instelling.”

- Veiligheid: vele mensen betrokken
- Centraal overleg
- Regelmaat

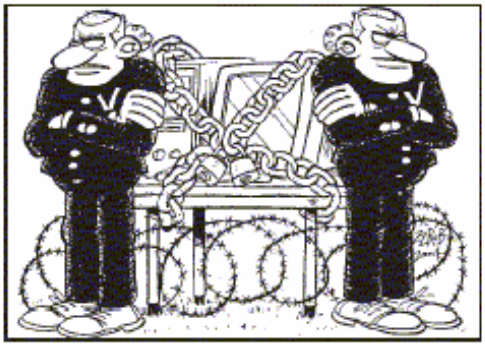
POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.3 Fysieke beveiliging en beveiliging van de omgeving

Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:

- de **toegang tot de gebouwen en lokalen beperken**
- **maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie ingeval van brand, inbraak of waterschade**.
- over een **alternatieve stroomvoorziening** beschikken



Zorg voor goede fysieke beveiliging van computerapparatuur

.be

4.3.1 Toegang tot gebouwen en lokalen

4.3.1. “de **toegang tot de gebouwen en lokalen beperken** tot de geautoriseerde personen en een **controle** erop verrichten zowel tijdens als buiten de werkuren.”

Collapsible gates with cross-lattice

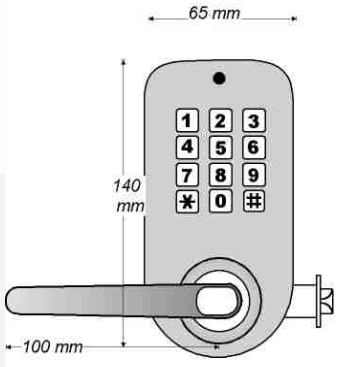
- OCMW heeft een publieke rol
- Badge, sleutel, loper
- Sociale controle
- Moeilijkheden

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Praktisch

- Inventariseren: wie heeft er toegang tot wat, wanneer en hoe?
- Moeilijkheden: verspreide locaties, oude (beschermde) gebouwen, deurpompen, evacuatie (personen: uit, hulpdiensten: in)
- Jullie ervaringen



Left hand lock

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.3.2 preventie, bescherming, detectie

4.3.2. “**maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie ingeval van brand, inbraak of waterschade**. “

- Basis: het fysisch in kaart brengen
- Eenvoudige fysische ingrepen
- Soorten inbraken, werkwijze inbreker

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Praktisch

- Inbraakvertraging!!! (ook met eenvoudige ingrepen)
- Methodologie: het fysisch in kaart brengen
- Soorten inbraken, werkwijze inbreker

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Praktisch

- Fysisch en discipline!
- Inbraakdetectiesysteem: code, valse alarmen, alternatieve doormelding, noodvoeding
- Serverlokaal:verluchting, temperatuur, deur, detectoren, brandpreventie, stof

4.3.3 alternatieve stroomvoorziening

4.3.3. “over een **alternatieve stroomvoorziening** beschikken waardoor de informaticaverwerkingen zonder risico kunnen worden afgesloten”

- UPS (uninterruptable power supply: ononderbreekbare stroomvoorziening)
- Doel: dataverlies voorkomen.
- Inventarisatie: servers, noodzakelijke randapparatuur => grootte UPS
- Productkeuze: software, service, plaatsing, testen, onderhoud
- Let op: sluit geen printers, faxen, lampen, luidsprekers aan op noodvoeding
- Onderhoud: alle noodvoedingen (server, alarm, telefooncentrale, noodverlichting, brandcentrale, …)

Uit de krant

De Morgen on line / telexberichten - Microsoft Internet Explorer provided by MERCURE for INTPMI

Meer en meer pc's besmet met schadelijke software (17/11 08:23)

(Belga) Meer en meer pc's worden besmet met schadelijke software die gebruikmaakt van de telefoonlijn om automatisch nummers te vormen die te veel aanrekenen. Vaak gaat het om nummers met de prefix 0903 (1,25 euro per minuut). Dat schrijft Le Soir woensdag.

Volgens de krant kan de factuur van de slachtoffers van de fraude oplopen tot meer dan 1.000 euro. Volgens Cécile Coppin, coördinator van internettoezicht bij Economische Zaken zijn er sinds het begin van het jaar meer dan 500 klachten binnengekomen, met een toename sinds juli. Vaak gebeurt het dat bij het surfen op het internet dergelijke programma's worden gedownload op de harde schijf van de gebruiker. Volgens een studie van antivirusuitgever Symantec in de Benelux - die volgende week verschijnt - is één computer op drie besmet met zo'n programma. (dwm) *(Belga)*

Microsoft bindt strijd aan tegen spyware

Microsoft brengt, op algemeen verzoek, een eigen programma op de markt dat de computer van zijn klanten beschermt tegen spyware. Maar of de uiteindelijke versie gratis zal zijn, valt nog af te wachten. 'We mogen onze marktpositie niet misbruiken', luidt het bij de softwaregigant.

Er is lang over gepalaverd geweest, en Microsoft heeft het zelfs al eens staalhard ontkend, maar sinds vorige week staat het er wel: een testversie van Microsofts antispyware-toepassing is vrijelijk te downloaden van de website van het bedrijf. Dat gebeurde een beetje op algemeen verzoek: Windows staat wereldwijd op zo'n 95 procent van alle computers geïnstalleerd, en nog eens zo'n 89 procent van diezelfde computergebruikers surft over het internet met Internet Explorer, de webbrowser van het bedrijf. En spyware komt bij uitstek binnen op pc's die onder die software draaien, omdat de makers van al die vuiligheid misbruik maken van 'gaten' in Windows en Explorer. "We moesten onze verantwoordelijkheid opnemen", zegt woordvoerder Frank De Graeve van Microsoft België. Spyware is in geen tijd een huizenhoog probleem geworden bij internetgebruikers. (RMe) (Eigen berichtgeving 05:25)

(c) EFA

4.4.1 toegang tot de gegevens

4.4 Logische toepassingsbeveiliging

4.4.1. "de **toegang tot de gegevens** nodig voor de toepassing en de uitvoering van de sociale zekerheid **beveiligen door middel van een identificatie-, authentificatie- en autorisatiesysteem."**

Identificatie : de gebruiker identificeren.

Authentificatie (=authenticatie): het controleren van iemands identiteit, voordat autorisatie gebeurt.

Autorisatie: op basis van een autorisatietabel (wie heeft er wanneer toegang tot wat) zal het systeem de geauthenticeerde gebruiker toegang geven tot bepaalde toepassingen/systemen/bestanden.

"Your logon password is XB#2D940. Write it down and don't lose it again."

Aanvallen

Password length	Time needed 26 characters per letter	Time needed 36 characters per letter	Time needed 52 characters per letter
1	325 nanoseconds	4.5 microseconds	6.5 microseconds
2	84 microseconds	0.16 milliseconds	0.34 milliseconds
3	2.2 milliseconds	5.83 milliseconds	0.017 seconds
4	0.057 seconds	0.21 seconds	0.91 seconds
5	1.49 seconds	7.55 seconds	47.53 seconds
6	38.61 seconds	4.53 minutes	41.18 minutes
7	16.73 minutes	2.72 hours	1.48 days
8	7.25 hours	4.08 days	77.34 days
9	7.86 days	146.93 days	11.01 years
10	204.23 days	14.48 years	572.58 years
11	14.54 years	521.35 years	29.77 millennia
12	378 years	18.77 millennia	1.55 million years

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Complexiteit

	L	a-z	L	a-z en 0-9 en A-Z	L	ASCII set
1		26		62		255
2		676		3.844		65.025
3		17.576		238.328		16.581.375
4		456.976		14.776.336		4.228.250.625
5		11.881.376		916.132.832		1.078.203.909.375
6		308.915.776		56.800.235.584		274.941.996.890.625
7		8.031.810.176		3.521.614.606.208		70.110.209.207.109.400
8		208.827.064.576		218.340.105.584.896		17.878.103.347.812.900.000
9		5.429.503.678.976		13.537.086.546.263.600		4.558.916.353.692.290.000.000
10		141.167.095.653.376		839.299.365.868.340.000		1.162.523.670.191.530.000.000.000
11		3.670.344.486.987.780		52.036.560.683.837.100.000		296.443.535.898.841.000.000.000.000
12		95.428.956.661.682.200		3.226.266.762.397.900.000.000		75.593.101.654.204.400.000.000.000.000
13		2.481.152.873.203.740.000		200.028.539.268.670.000.000.000		19.276.240.921.822.100.000.000.000.000.000
14		64.509.974.703.297.200.000		12.401.769.434.657.500.000.000.000		4.915.441.435.064.640.000.000.000.000.000.000
15		1.677.259.342.285.730.000.000		768.909.704.948.767.000.000.000.000		1.253.437.565.941.480.000.000.000.000.000.000.000
16		43.608.742.899.428.900.000.000		47.672.401.706.823.500.000.000.000.000		319.626.579.315.078.000.000.000.000.000.000.000.000
17		1.133.827.315.385.150.000.000.000		2.955.688.905.823.060.000.000.000.000.000		81.504.777.725.345.000.000.000.000.000.000.000.000.000
18		29.479.510.200.013.900.000.000.000		183.252.712.161.030.000.000.000.000.000.000.000		20.783.718.319.963.000.000.000.000.000.000.000.000.000.000
19		766.467.265.200.362.000.000.000.000		11.361.668.153.983.800.000.000.000.000.000.000.000		5.299.848.171.590.560.000.000.000.000.000.000.000.000.000.000
20		19.928.148.895.209.400.000.000.000.000		704.423.425.546.998.000.000.000.000.000.000.000.000		1.351.461.283.755.590.000.000.000.000.000.000.000.000.000.000.000
	10	ditwaslaat	8	31Bavo50	6	ç92dr5
	15	ditwashetmeeste	12	31Bavo50Woef	9	ç92dr5(%x
	20	ooitwasdithetmeeste	16	31Bavo50WoefSlim	12	ç92dr5(%xg3é

POD Maatschappelijke Integratie
SPP Intégration Sociale

.be

Wachtwoordbeleid

- Belang van wachtwoordbeleid
- Complexiteit wachtwoord (wachtzin)
- Memoriseren wachtwoord
- Wijzigen wachtwoord
- Op papier in kluis?
- In tabel sociale software leesbaar?
- Juridisch
- Mogelijkheden e-ID of eIK of elektronische identiteitskaart

Elektronische identiteitskaart

4.4.2 veiligheidskopieën

4.4.2. “een systeem van regelmatig te controleren **veiligheidskopieën (back-up)** invoeren **om**, ingeval 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 m.b.t. de toepassingen en het besturingssysteem).”

Waarom?

- netwerk van de sociale zekerheid: gegevens decentraal
- **gegevens over uw OCMW klanten** : enkel bij u bewaard
- **gegevensverlies** bij u: gevolgen
- **ook over de gegevens van toepassingen en besturingssystemen**
- Bij ramp: van niets terug volledig operationeel geraken.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Media rotatie schema

weekdag	MediumNr	Week 1	MediumNr	Week 2	MediumNr	Week 3	MediumNr	Week 4	MediumNr	Week 5
maandag	1	Dagelijkse incrementele back-up	7	Dagelijkse incrementele back-up	1	Dagelijkse incrementele back-up	7	Dagelijkse incrementele back-up	1	Dagelijkse incrementele back-up
dinsdag	2	Dagelijkse incrementele back-up	8	Dagelijkse incrementele back-up	2	Dagelijkse incrementele back-up	8	Dagelijkse incrementele back-up	2	Dagelijkse incrementele back-up
woensdag	3	Dagelijkse incrementele back-up	9	Dagelijkse incrementele back-up	3	Dagelijkse incrementele back-up	9	Dagelijkse incrementele back-up	3	Dagelijkse incrementele back-up
donderdag	4	Dagelijkse incrementele back-up	10	Dagelijkse incrementele back-up	4	Dagelijkse incrementele back-up	10	Dagelijkse incrementele back-up	4	Dagelijkse incrementele back-up
vrijdag	5	Dagelijkse volledige back-up	11	Dagelijkse volledige back-up	5	Dagelijkse volledige back-up	11	Dagelijkse volledige back-up	5	Dagelijkse volledige back-up
	6	Back-up Informatica-omgeving	12	Back-up Informatica-omgeving	6	Back-up Informatica-omgeving	12	Back-up Informatica-omgeving	6	Back-up Informatica-omgeving
	I	Wekelijkse Back-up 1	II	Wekelijkse Back-up 2	III	Wekelijkse Back-up 3	IV	Wekelijkse Back-up 4	V	Wekelijkse Back-up 5

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.4.3 loggingsysteem

4.4.3. "een **loggingsysteem implementeren voor de persoonsgegevens** nodig voor de toepassing en uitvoering van de sociale zekerheid."

Wat?

- Logging: historische data (wie, wat, wanneer)

Waarom?

- Rol veiligheidsconsulent
- Ook nuttig ter bestrijding van virussen e.d.

! Integriteit logfile: lokaal en voor sociale software

Let op: een beleid voor het bewaren van de loggings moet ook opgesteld worden

Het veel gebruikte SYSLOG heeft veel zwakke punten: blz 2-5 in www.giac.org/practical/GSEC/Kenneth_Nawyn_GSEC.pdf

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.4.4 Veiligheidsinbreuken detecteren

4.4.4. "**een systeem en formele, geactualiseerde procedures** installeren die toelaten om **veiligheidsinbreuken te detecteren, op te volgen en te herstellen.**"

- **Manuele taken**: bekijken van logfiles, bekijken van internetverkeer
- **Opvolgen** van veiligheidsinbreuken
- **Herstellen** van veiligheidsinbreuken

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.4.5 relatie prefixgedeelte – identiteit gebruiker

4.4.5. “Wanneer de instelling in de zone “USERID” van het prefixgedeelte van een bericht aan de Kruispuntbank, het programmanummer overneemt dat aan de basis ligt van het bericht dat ze naar de Kruispuntbank stuurt (...) **In dat geval moet het OCMW dus zelf de relatie leggen tussen het programmanummer dat ze overneemt in het prefixgedeelte van het bericht dat zij naar de Kruispuntbank stuurt en de identiteit van de natuurlijke persoon die het bericht verstuurt**.”

Wat?

Het OCMW dient ervoor te zorgen dat de Kruispuntbank steeds achteraf te weten kan komen welke natuurlijke persoon elektronisch berichten heeft uitgewisseld met hen.

Waarom?

Om in geval van problemen te weten wie aan de oorzaak lag.

Hoe?

Via uw programma om te communiceren met de Kruispuntbank. De veiligheidsconsulent moet altijd een inventaris bijhouden van de identiteiten van de gebruikers om de gebruikersnummers en de namen te kunnen laten overeenstemmen.

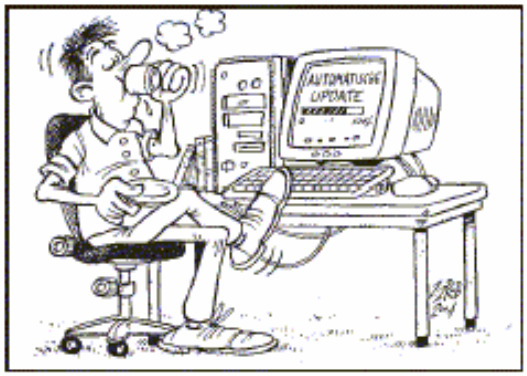
4.5 De toepassingen

4.5. Ontwikkeling, productie en onderhoud van toepassingen

Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:

4.5.1. 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.

4.5.2. **over formele en geactualiseerde procedures beschikken voor de uitwerking van documentatie bij de ontwikkeling van nieuwe en het onderhoud van bestaande toepassingen en systemen.**



Installeer tijdig softwarereparaties (verkregen van een betrouwbare bron)

procedures

4.5.1. 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.

4.5.2. **over formele en geactualiseerde procedures beschikken voor de uitwerking van documentatie bij de ontwikkeling van nieuwe en het onderhoud van bestaande toepassingen en systemen.**

Escrow clausule

- Broncode van de software bij een tussenpersoon deponeren
- Bij failliet of andere in gebreke stelling opvraagbaar
- Bij notaris of speciaal bedrijf
- Check of het werkt!
- Voor elke nieuwe versie nieuwe deponering

4.6.1 toegang beperken en veiligheidsinbreuken detecteren

4.6 Netwerkbeveiliging

4.6.1. **Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:**

4.6.1.1. de **toegang tot het (de) informaticasyste(e)m(en) beperken** tot geïdentificeerde, geauthentifieerde en geautoriseerde personen/objecten

4.6.1.2. een **systeem en formele, geactualiseerde procedures installeren die toelaten om veiligheidsinbreuken te detecteren, op te volgen en te herstellen**.

Informaticasystemen: de apparaten en de fysische computers die worden gebruikt om de gegevens te verwerken

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

4.6.3 Secundaire net

4.6.3. De **socialezekerheidsinstellingen van het secundaire net <u>kunnen</u>** 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 **secundaire netwerkinstellingen veiligheidsmaatregelen implementeren die in overeenstemming zijn en blijven met de maatregelen getroffen op het niveau van het Extranet van de sociale zekerheid**

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Firewall

- Onbeschermde PC wordt in 20 minuten gekaapt
- Aansprakelijkheid bestuur: het niet nemen van beschermingsmaatregelen is ook strafbaar! (let zeker op bij draadloze netwerken)

Platform	Total attacks	Attacks / day	Attacks / hour
XP SP1	139,024	8,177	341
OS X	138,647	8,155	339
Win SBS	25,222	1,400	61
XP SP2	1,386	82	3.4
XP with ZoneAlarm	848	50	2.1
Linspire	795	46	1.9

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

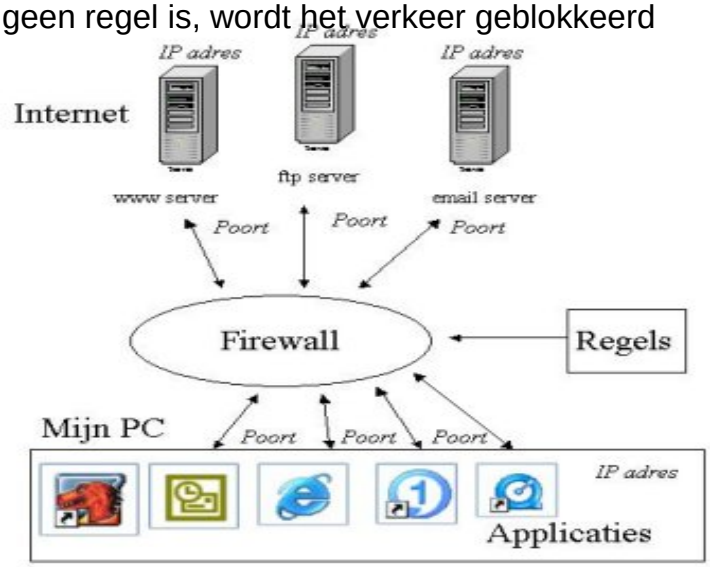
Firewall werking helikopterview

Een firewall filtert op basis van een set regels al het inkomende en uitgaande verkeer.

Een regel beschrijft welke lokaal draaiende applicatie op welke poort mag communiceren met een server (www, ftp, email etc.) op het internet.

Op het moment dat er van buiten naar binnen, of van binnen naar buiten een connectie opgezet wordt, wordt door de firewall gecontroleerd of er een regel in de database is, die dat verkeer toestaat.

Als er geen regel is, wordt het verkeer geblokkeerd



POD SPP Maatschappelijke Integratie Intégration Sociale

.be

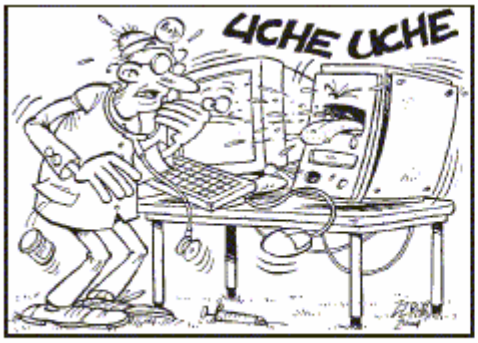
4.9 Virussen

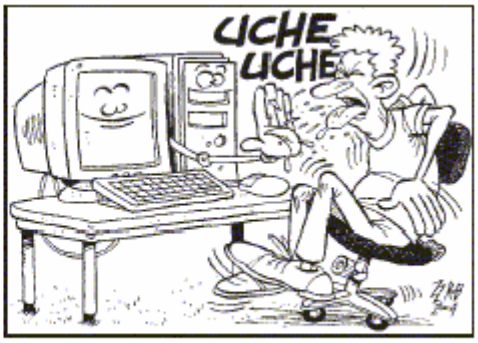
4.9. Bescherming tegen virusinfecties

Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:

4.9.1. over een **gebruikershandleiding beschikken m.b.t. het voorkomen van virusbesmettingen**, het gebruik van de geïnstalleerde antivirussoftware en de te treffen acties ingeval van virusinfectie.

4.9.2. een **geactualiseerde antivirussoftware installeren** teneinde virusinfecties te voorkomen, te detecteren en te corrigeren.





Installeer een virusscanner en houdt deze up to date

Virusbestrijding en andere

- Bronnen van virussen
- Kettingbrieven
- **Spyware**
- Hoaxes
- Macro-virussen
- *Voorkomen is beter dan genezen*
  - Zorg dat je besturingssysteem en software up-to-date zijn.
  - Zorg ervoor dat er een recente virusscanner (en virusdefinitiebestanden) op je systeem staat
  - Regelmatig (liefst automatisch) virusscan uitvoeren
  - Controleer alvorens te openen/downloaden/installeren

Acties bij besmetting:

- raak niet in paniek, zet je werkstation NIET uit, noteer wat je hebt gezien, voorkom verdere verspreiding, waarschuw (niet via e-mail) de systeembeheerder / lokale pc-beheerder, gebruik je werkstation niet totdat deze weer 'ontsmet' is, ga niet op een ander werkstation met je diskettes/memorystick aan het werk, breng je omgeving, op de hoogte, liefst telefonisch.

De beheerder:

- het virus proberen te detecteren, de virusscanner kan sommige virussen zelf verwijderen, op de website (via een andere PC) van de leverancier van je virusscanner, informatie over het verwijderen van het virus, al je diskettes virusvrij maken, schade die niet met ontsmetten te herstellen is via back-ups proberen ongedaan te maken, nagaan op welke wijze besmetting heeft kunnen optreden

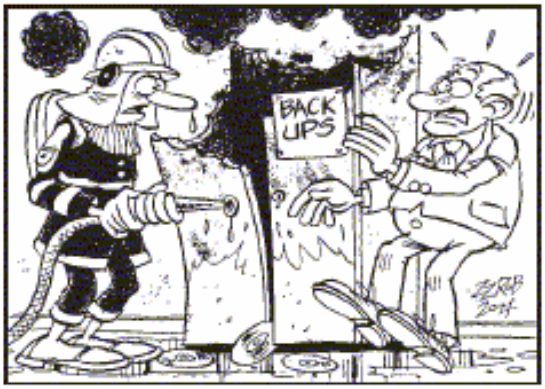
E-mail/internet gebruik

- Gebruik, doelgroep
- Misbruik
- Contrôle/controlesoftware
- Heksenjacht
- Digitale handtekening/Encryptie
- Sancties: top-down, escalatie, statuut persoon
- Netiquette
- Rechtspraak
- Er kan veel voorkomen worden door zaken onmogelijk te maken voor de gebruiker

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Continuïteitsplan



Maak en test regelmatig een backup en bewaar deze op een veilige plek

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Inventaris

4.8. Inventaris

Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet over een **permanent bijgewerkte inventaris beschikken**

van het informaticamateriaal en software.

Inventaris= wat gebruiken we nu en waarvoor?

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Risico-analyse

4.7.1. een **risico-analyse uitvoeren** teneinde de uitwerking van een continuïteitsplan mogelijk te maken.

kwetsbaarheden die - bij **ramp -**het OCMW hinderen

maatregelen om te bekomen dat - in geval van **ramp** - het **OCMW kan herbeginnen werken na x dagen**

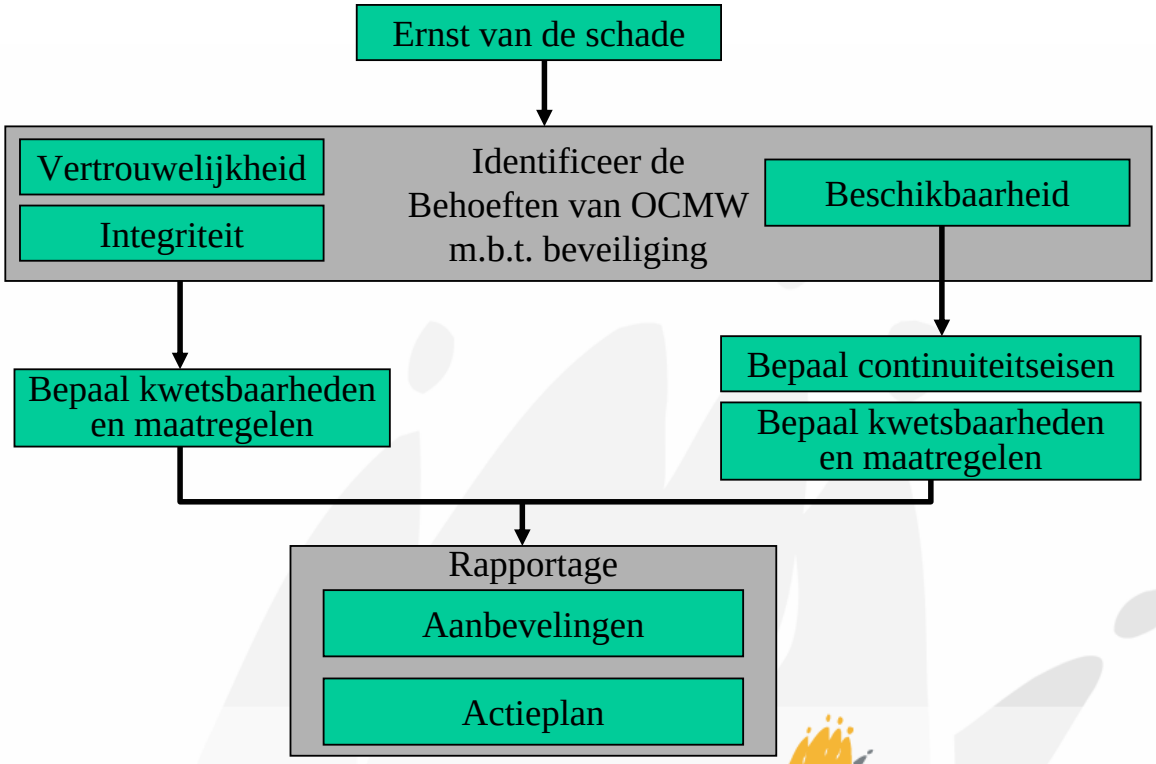
Risico's ordenen

=>zicht krijgen op de kosten-baten van investeringen in beveiliging.

POD SPP Maatschappelijke Integratie Intégration Sociale

.be

Schema



Continuïteitsplan

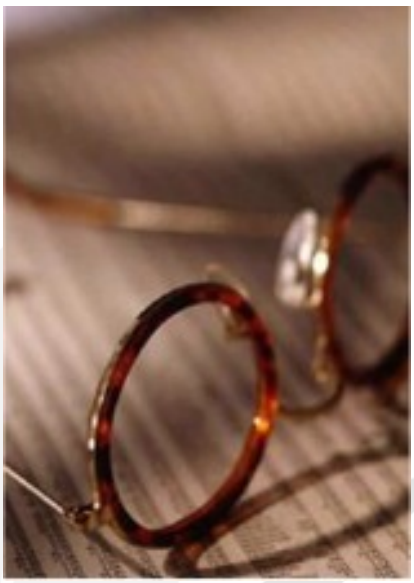
4.7.2. een **continuïteitsplan uitwerken**, testen en onderhouden teneinde de opdrachten inzake sociale zekerheid van de instelling te kunnen waarborgen. **Tevens moet zij in een informatica-uitwijkcentrum voorzien ingeval van beperkte of totale ramp.**

Continuïteitsplan: richt zich specifiek op de situatie na een calamiteit en dient antwoord te geven op de vraag: "Hoe nu verder?".

Informatica-uitwijkcentrum: de gemeente van wie het OCMW afhangt heeft vaak vele gebouwen. In een uitwijkcentrum kunnen tijdelijk de activiteiten van het OCMW opnieuw opgestart worden.

4.10.Toezicht/audit

Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet **tenminste één keer om de vier jaar een audit organiseren met betrekking tot de situatie van de logische en fysieke veiligheid**.

Mutueel

Checklist