

**OCMW X****INFORMATIEVEILIGHEIDSBELEID****1. Inleiding**

---

De informatisering van de instellingen van de sociale zekerheid en de toenemende samenwerking inzake informatiebeheer, cfr de aansluiting van de instellingen van de sociale zekerheid op het netwerk van de kruispuntbank, biedt uitzicht op enorme verbeteringen op het vlak van effectiviteit en efficiëntie. Maar tegelijkertijd worden nieuwe risico's gelopen.

De afzonderlijke instellingen van de sociale zekerheid zijn immers niet langer op zichzelf staande informatieverwerkende eenheden, maar onderdelen van een samenhangende groep. Door de groeiende samenwerkingsverbanden wordt de kans op en omvang van gereflecteerde schade op andere systemen dan waar de basisschade zich voordoet veel groter. De visie inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer dient dan ook te worden vastgelegd. De uitvoering ervan in elke instelling van de sociale zekerheid behoort tot de basisverantwoordelijkheid van elke eind verantwoordelijke van deze dienst.

**2. Basisbeginselen**

---

De informatieveiligheid bestaat uit de preventie van schade die kan worden toegebracht aan de goede werking van de instellingen van de sociale zekerheid en de dienstverlening aan haar gebruikers, door de aantasting van haar middelen en procedures van (elektronische) informatieverwerking. Het uiteindelijk te beschermen voorwerp, en met name de goede werking van de instellingen van de sociale zekerheid en de persoonlijke levenssfeer van alle betrokkenen, is van uitzonderlijk belang. Gepaste maatregelen zijn dan ook nodig voor het waarborgen van de integriteit, de beschikbaarheid, de vertrouwelijkheid, de niet-weerlegbaarheid, de authenticiteit en de auditeerbaarheid van de informatie en de informatieverwerkende systemen.

Het voorkomen van schade die kan worden toegebracht aan de goede werking van de informatiesystemen van de instellingen van de sociale zekerheid enerzijds en aan de persoonlijke levenssfeer van de betrokkenen anderzijds moet op de eerste plaats komen. Preventie is namelijk de beste manier van beveiligen. Het is de actie die vermijdt dat de schade optreedt, door het tijdig opmerken en wegnemen van de bedreigingen. Primaire preventie gaat voor secundaire en tertiaire preventie, die respectievelijk de reeds aangerichte schade herstellen en verhinderen dat de opgelopen schade nog verergert. Toch zijn de drie vormen van preventie nodig, omdat niet alle schade kan vermeden worden, ook niet bij het beste informatieveiligheidsbeleid. Bij het vastleggen van een veiligheidsbeleid is het nodig deze indeling in het oog te houden, daar ze aan het licht brengt dat sommige eenvoudige en weinig kostelijke maatregelen een groter gewicht hebben dan dure maar minder efficiënte acties.

Dit brengt ons tot een volgend veiligheidsbeginsel, namelijk dat van de risico-afweging. Elke vooruitgang en vernieuwing is het resultaat van het opzoeken van goede risico's en het vermijden van slechte. Het wikken van de goede en de slechte risico's vergt een beredeneerde benadering: de kansen op het verwerven van winst moeten de kansen op het lijden van schade in aanzienlijke

mate overtreffen. Door het opdrijven van de beveiliging kan voor een positieve balans worden gezorgd, maar ook de beveiliging brengt kosten mee die winst ernstig kunnen aantasten. De kansen op schade moeten weliswaar steeds zo klein mogelijk gehouden worden, maar tegen een redelijke prijs. De inspanningen inzake informatieveiligheid moeten dan ook gericht zijn op het bereiken van een redelijk evenwicht tussen het behalen van de winst- en het vermijden van de verlieskansen, die uit vernieuwende actie voortvloeien. Absolute veiligheid mag niet voorgesteld worden als een na te streven ideaal. Anders dreigt elke vernieuwing in de kiem te worden gesmoord.

De beveiliging van een informatiesysteem is geen technisch produkt, dat door deskundigen in het systeem kan worden ingebouwd, maar volgt uit de zorgzame uitvoering van de dagelijkse opdracht van iedere persoon die bij de werking ervan betrokken is. Wie zich een veilige toekomst wil verzekeren, moet in de eerste plaats zelf voor zijn beveiliging zorgen. Daarom is het wenselijk veiligheid op te nemen als waarde in het waardenkader van elke medewerker van de instellingen van de sociale zekerheid, als een goed dat permanent moet worden nagestreefd.

Een deskundige kan enkel raad geven, hulpmiddelen aanwijzen, toezicht houden, motiveren, aandacht trekken, oog en oor zijn voor de gevaren waaraan de bedienaars van het te beschermen systeem zijn blootgesteld. De beveiliging zelf moet hij overlaten aan hen die het systeem bedienen. Zij en niemand anders dragen dan ook de eerste verantwoordelijkheid voor de bescherming van het systeem. De sociale organisatie van de beveiliging is daarom een *conditio sine qua non* van gelijk welk veiligheidssysteem. Zelfs de beste technologische hulpmiddelen kunnen nooit de sociale controle vervangen. Zij kunnen het veiligheidsniveau ongetwijfeld verbeteren, maar in laatste instantie berust veiligheid op een efficiënte organisatie.

Een informatiesysteem is zo veilig als zijn zwakste schakel. Een homogeen geheel van maatregelen is nodig, zoniet zijn de inspanningen zinloos. Daarom zijn maatregelen nodig op organisatorisch, juridisch, technisch en fysisch vlak. De veiligheidsproblematiek dient bovendien op een gestructureerde wijze aangepakt te worden en omvat in hoofdzaak de volgende fasen: de inventarisatie van de bestaande beveiligingssituatie, het vastleggen van prioriteiten in een veiligheidsbeleid, het concreet vertalen van het veiligheidsbeleid naar maatregelen vastgelegd in een veiligheidsplan, het implementeren van de geplande maatregelen, en het voortdurend toetsen of de bestaande maatregelen nog wel nodig zijn en worden nageleefd.

Het voorstellen van een omnivalente modeloplossing inzake informatieveiligheid is onmogelijk. Een onderscheid dient te worden gemaakt tussen de algemene doelstellingen, die globaal kunnen worden vastgelegd, en de manier waarop deze doelstellingen worden gerealiseerd. Bij de keuze van de manier waarop de doelstellingen worden gerealiseerd dient voldoende ruimte te worden gelaten om optimaal in te spelen op de concrete behoeften en risico's van elke omgeving. Responsabilisering van de betrokkenen via het opleggen van gecontroleerde zelfregulering werkt in dit kader efficiënter dan overnormering van bovenuit.

Veiligheid kan efficiëntie en gebruiksvriendelijkheid belemmeren en kost geld. Bovendien vernietigt de beste preventie, met name de primaire, de bewijzen van haar efficiëntie. Zij laat immers de schade niet ontstaan. Dit veroorzaakt mettertijd een valse indruk van nutteloosheid, gevolgd door verslapping van de aandacht en van de inspanning. Daarom is een volgehouden motivatie en sensibilisatie en de permanente investering in informatieveiligheid onontbeerlijk. Tegen het bijna wetmatig verval van de preventieve inspanning moet permanent en zeer bewust worden ingegaan. Dit vergt een voortdurende opvijzeling van de veiligheidsmoraal, zowel bij het kaderpersoneel als bij hun ondergeschikten.

Het informatieveiligheidsbeleid moet tenslotte conform zijn aan de geldende regelgeving, o.a. inzake de bescherming van de persoonlijke levenssfeer of de elektronische handtekening.

De vormgeving van de informatieveiligheid geschiedt op basis van internationaal aanvaarde ISO-normen; in casu is vooral de ISO-norm 17799 (Code of practice inzake informatieveiligheid) van groot belang en zal in dit informatieveiligheidsbeleid gehanteerd worden.

### **3. De verdere uitbouw overeenkomstig de ISO-norm 17799**

De verdere structuur van dit informatieveiligheidsbeleid is opgebouwd overeenkomstig de hoofddomeinen van beveiliging voorzien in de ISO-norm 17799, aangevuld met bijzondere maatregelen inzake de verwerking van persoonsgegevens en de externe communicatie inzake het informatieveiligheidsbeleid.

De domeinen van beveiliging voorzien in de ISO-norm 17799 zijn:

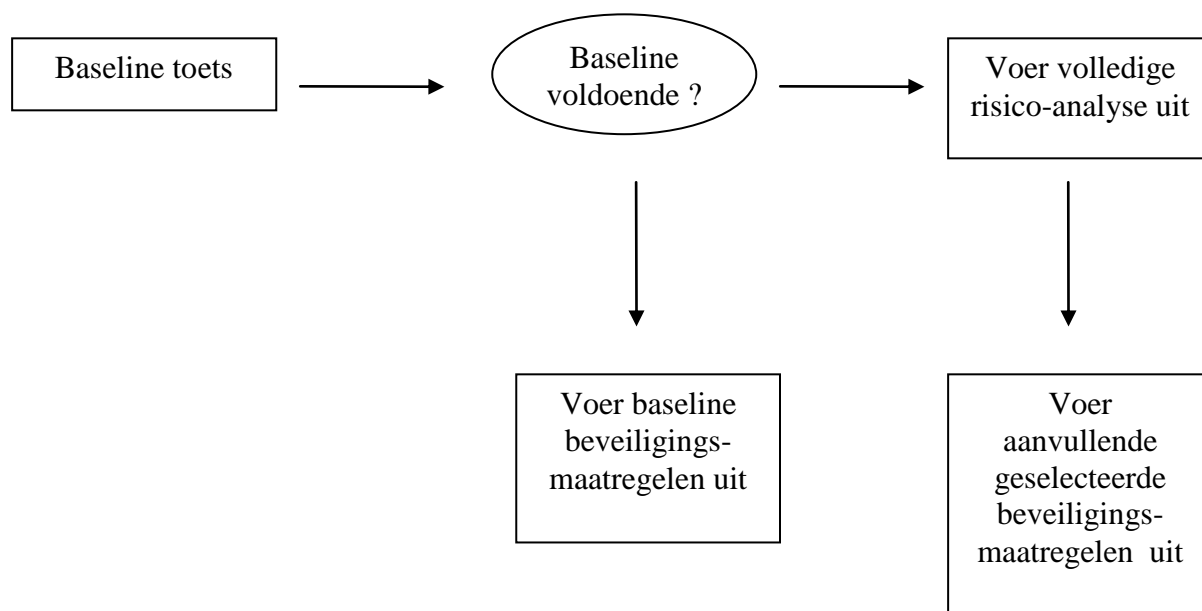
- Organisatie
- Beleid
- Classificatie van de informatie
- Beveiligingseisen t.a.v. het personeel
- Fysieke beveiliging van de omgeving
- Beheer van de communicatie processen
- Verwerking van persoonsgegevens
- Toegangsbeveiliging
- Continuïteitsmanagement
- Interne en externe controle op naleving

De ISO-norm 17799 noemt 3 bronnen voor het opstellen van prioriteiten:

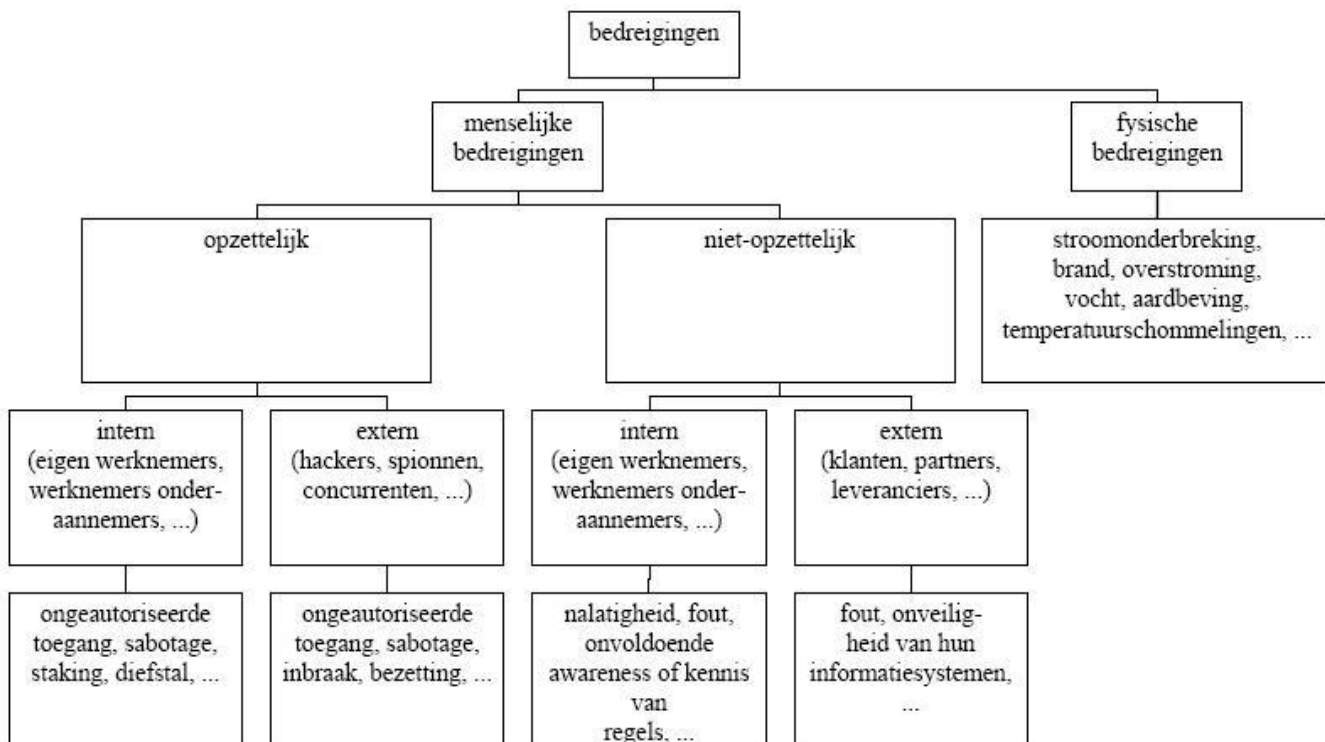
- de inschatting van de grootste risico's;
- de externe conformiteitsanalyse, met name de conformiteit met datgene wat wordt voorgeschreven door de wet of de contracten en wat goed gebruik is in de sector;
- de interne conformiteitsanalyse, met name de gevolgen voor de informatiesystemen en hun veiligheid die voortvloeien uit de evoluerende bedrijfsdoelstellingen

Om prioriteiten te stellen, wordt aangeraden een baseline-toets door te voeren. Dit houdt in dat per informatiesysteem wordt nagegaan of een aantal baselinemaatregelen voldoende worden geacht als beveiligingsmaatregelen in functie van de drie vermelde bronnen. Enkel indien deze baseline-maatregelen niet voldoende lijken, wordt voorgesteld een gedetailleerde risico-analyse uit te voeren.

In volgend schema wordt deze methode schematisch weergegeven:



Bij het uitvoeren van de risico-analyse voor de informatiesystemen waarvoor de baselinemaatregelen niet volstaan, moeten de twee risico-aspecten, de mogelijke schade door een incident en de waarschijnlijkheid van een incident, worden afgezet tegen de kost van de maatregelen om het risico te vermijden. De waarschijnlijkheid van een incident vloeit voort uit de mogelijke bedreigingen.



Een gedetailleerde risico-analyse is voor de instellingen van de sociale zekerheid gewenst in volgende gevallen:

- voor informatie en informatiesystemen die voor de instellingen van de sociale zekerheid een bijzonder belang hebben, te weten
  - informatiesystemen die gebruikt worden bij de verwerking van de als vitaal, kritisch, geheim of vertrouwelijk informatie
- in situaties waarin een beveiligingsincident de volgende gevolgen kan hebben
  - een ernstige aantasting van het vertrouwen in de instelling van de sociale zekerheid;
  - gevaar voor de veiligheid van de eigen medewerkers, externe personen of groepen;
  - ernstige vermindering van de dienstverlening aan burgers en ondernemingen;
- in situaties waarin de schade van een eventueel incident groter is dan een te bepalen geldbedrag.

#### **4. Aanpak per domein van de ISO-norm 17799**

---

##### **4.1. Organisatie**

---

- een veiligheidsconsulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer wordt aangeduid in elke instelling van de sociale zekerheid; voor kleinere instellingen van de sociale zekerheid is een gezamenlijke consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer mogelijk; de consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer heeft een duidelijk functieprofiel (o.a. de taken van de aangestelde voor de gegevensbescherming in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna genoemd Wet Verwerking Persoonsgegevens), en een adviserende, documenterende, sensibiliserende en intern auditerende taak inzake informatieveiligheid); hij/zij heeft een gereguleerd statuut, dat een onafhankelijke taakuitvoering waarborgt (zie het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid, B.S., 21 augustus).
- Minimale veiligheidsnormen die moeten nageleefd worden door de sociale instellingen met het oog op hun aansluiting op het netwerk van de Kruispuntbank van de Sociale Zekerheid
- Het bestuur is zich bewust van de ethische gedragscode voor de veiligheidsconsulent en de deontologische regels m.b.t. onder meer:
  - zijn objectiviteit, onpartijdigheid en onafhankelijkheid;
  - zijn professionele ingesteldheid;
  - zijn loyaliteit ten opzichte van zijn werkgever;
  - het interdisciplinair en vertrouwelijk karakter van zijn functie.

- De instelling van de sociale zekerheid verbindt zich ertoe de nodige informatie te verstrekken aan de veiligheidsconsulent, zodanig dat hij/zij over de gegevens beschikt voor de uitvoering van de hem toegewezen veiligheidsopdracht
- De gegevens en bereikbaarheid van de veiligheidsconsulent worden meegedeeld aan elke medewerker van de instelling van de sociale zekerheid

#### **4.2. Beleid**

---

- via een systeem van stapsgewijze verfijning, worden policies, richtlijnen, architectuur, standaarden, procedures en technieken ter concretisering van het informatieveiligheidsbeleid vastgelegd. De policies zouden telkens de volgende structuur kunnen hebben:
  - materieel toepassingsgebied: waarover handelt de policy;
  - personeel toepassingsgebied: op wie is de policy van toepassing;
  - definities van de begrippen gehanteerd in de policy;
  - algemene principes: vaststelling van regels en verantwoordelijkheden;
  - vereisten en verwijzingen naar andere policies;
  - sancties, o.a. voortvloeiend uit reglementering, bij niet-naleving van de policy;
  - verwijzing naar richtlijnen, architectuur, procedures, standaarden en technieken om de policy na te leven;

#### **4.3. Classificatie van de informatie**

---

- het doel van de classificatie is het bepalen van het vereiste beschermingsniveau van elk stukje informatie, rekening houdend met twee dimensies
  - de belangrijkheid voor de continuïteit van de werking van en de dienstverlening door de instelling van de sociale zekerheid (indeling in bijvoorbeeld vitaal, kritisch, nodig, nuttig);
  - de gevoeligheid in het licht van de bescherming van de persoonlijke levenssfeer (indeling in bijvoorbeeld publiek, intern, vertrouwelijk, geheim);
- het toepassingsgebied van de classificatie betreft de informatie (vnl. persoonsgegevens) gebruikt voor de dienstverlening aan burgers, ondernemingen en ambtenaren, ongeacht de drager waarop ze worden bewaard

#### **4.4. Beveiligingseisen t.a.v. het personeel**

---

- de beveiligingstaken en –verantwoordelijkheden worden opgenomen in alle functie-omschrijvingen waarvoor dit relevant is; als gevoelig beschreven functies worden als dusdanig aangeduid in de functie-omschrijving

- sollicitanten voor gevoelige functies worden gescreend
  - er wordt gezorgd voor awareness, opleiding en training van alle medewerkers inzake informatiebeveiliging en bescherming van de persoonlijke levenssfeer
  - er worden procedures vastgelegd voor de rapportering van informatieveiligheidsincidenten en ernstige informatieveiligheidsrisico's aan de consultant inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer
  - er wordt een werkwijze vastgelegd om de gemelde incidenten en risico's door de consultant inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer te laten analyseren en passende maatregelen voor te stellen
- er wordt voor gezorgd dat de (disciplinaire) sancties bij niet-naleving van of inbreuk op maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer voldoende bekend zijn.

#### **4.5. Fysieke beveiliging van de omgeving**

---

- er zijn ruimten beschikbaar die goed beveiligd zijn tegen onrechtmatige beïnvloeding van buitenuit, onrechtmatige toegang, inbraak, water, brand, ... en de ICT-middelen die kritische bedrijfsprocessen ondersteunen zijn ondergebracht in deze ruimten
- de stroomvoorziening voor ICT-middelen die kritische bedrijfsprocessen ondersteunen is gewaarborgd
- kabels en golven zijn beveiligd, in het bijzonder tegen aftappen

#### **4.6. Beheer van de communicatie processen**

---

- er zijn preventieve maatregelen voor beveiliging van alle informatiesystemen tegen virussen en kwaadaardige software
- procedures voor de omgang met informatiedragers (tapes, diskettes, cassettes, ...) zijn vastgelegd en worden nageleefd, met o.a. regels inzake
- de opslag en toegang ertoe;
  - het transport;
  - de vernietiging;
- netwerken worden beheerd volgens procedures, vooral wanneer ze gekoppeld worden met externe netwerken; daarbij wordt o.a. aandacht besteed aan
- scheiding van interne en externe netwerken;
  - periferiebeveiliging van interne netwerken (firewalls, ...);
  - authenticatie van componenten t.o.v. mekaar;
  - intrusion detection;
  - toepassing van encryptietechnieken waar nodig;

#### **4.7. Verwerking van persoonsgegevens**

---

- de persoonsgegevens in het algemeen worden verwerkt overeenkomstig de beginselen vervat in de Wet Verwerking Persoonsgegevens
  - doelgebondenheid: persoonsgegevens worden slechts verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden; de doeleinden van de verdere verwerking zijn verenigbaar met de doeleinden van de initiële verwerking;
  - evenredigheid: de verwerkte persoonsgegevens zijn toereikend, ter zake dienend en niet overmatig in functie van de doeleinden van de verwerking;
  - nauwkeurigheid: de verwerkte persoonsgegevens worden, indien nodig, bijgewerkt, verbeterd of gewist;
  - redelijke bewaarduur: de persoonsgegevens worden niet langer bewaard dan nodig voor de verwezenlijking van de doeleinden van de verwerking;
  - de gevoelige persoonsgegevens, gezondheidsgegevens en gerechtelijke persoonsgegevens worden verwerkt overeenkomstig de bijzondere regelen terzake vastgelegd in de Wet Verwerking Persoonsgegevens

#### **4.8. Toegangsbeveiliging**

---

- identificatie- en authenticatiemiddelen (user-id/paswoord, token, digitaal certificaat, elektronische handtekening, ...) worden vastgelegd voor mensen, fysieke resources en toepassingen
- gebouwen worden gesegmenteerd, beveiligingsringen worden aangebracht en toegangscontrolemaatregelen tot plaatsen worden geïmplementeerd
- toegangscontrolemaatregelen tot fysieke resources (computers, kasten, netwerken, ...) door gebruikers (mensen of andere fysieke resources) worden geïmplementeerd, met bijzondere aandacht voor persoonsgebonden bedrijfsmiddelen (vb. laptop's, handhelds, mobiele telefoons, ...)
- toegangscontrolemaatregelen tot toepassings(onderdelen) en diensten(onderdelen) door interne en externe gebruikers (mensen of andere toepassingen of diensten) worden geïmplementeerd
- ICT-middelen worden automatisch geblokkeerd na een periode van inactiviteit
- alle toegangen en uitgevoerde handelingen worden gelogd

#### **4.9. Continuïteitsmanagement**

---

- back-upprocedures voor toepassingen en informatie worden schriftelijk vastgelegd en toegepast
- een continuïteitsplan voor het hele informatiesysteem wordt schriftelijk vastgelegd en ter beschikking gesteld van alle betrokkenen
  - te beginnen met de vitale en kritische componenten en processen;
  - met een inventaris van de benodigde middelen en competenties voor elke component en elk proces;
  - met een beschrijving van de acties, de verantwoordelijkheden en de procedures bij noodsituaties (ter plaatse of elders);
  - met een beschrijving van de vervolgacties en –procedures bij noodsituaties om de normale bedrijfsvoering te herstellen;
  - met een beschrijving van de scenario's voor het testen van het continuïteitsplan met de betrokken derden;

#### **4.10. Interne en externe controle op naleving**

---

- de controlemiddelen en de te controleren informatiesystemen en loggings zijn eenvoudig toegankelijk voor de interne en externe controle
- systemen worden beschikbaar gesteld voor de consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer, die permanent mogelijke inbreuken op de wetgeving, de policies, de richtlijnen, de architectuur, de procedures en de standaarden en op ongewenst gebruik van de ICT-voorzieningen aan de orde stellen
- elke verantwoordelijke van een verwerking van persoonsgegevens ziet regelmatig toe op de naleving van de in de overeenkomsten vastgelegde veiligheidsmaatregelen door de eventuele verwerkers van persoonsgegevens

### **5. Bijlage : wetgeving in verband met informatieveiligheid**

---

- Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid (Belgisch Staatsblad van 21 augustus 1993)
  - Gewijzigd bij het koninklijk besluit van 8 oktober 1998 (Belgisch Staatsblad van 24 december 1998)

- Minimale veiligheidsnormen die moeten nageleefd worden door de sociale instellingen met het oog op hun aansluiting op het netwerk van de Kruispuntbank van de Sociale Zekerheid
  - Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens
  - Koninklijk besluit van 4 februari 1997 tot organisatie van de mededeling van sociale gegevens van persoonlijke aard tussen instellingen van de sociale zekerheid.
-