

ISMS

(Information Security Management System)

Minimale Normen

Versie 2011

Opmerking: in dit document zijn de opmerkingen verwerkt van een werkgroep waaraan de volgende personen hebben deelgenomen: de heren Bochart (KSZ), Costrop (Smals), Noël (KSZ), Petit (FBZ), Quewet (FOD Volksgezondheid), Symons (RVA), Van Cutsem (RSZPPO), Van der Goten (RIZIV).

Inhoudstafel

| | | |
|------|--|----|
| 1. | VOORBESCHOUWING | 3 |
| 2. | TOEPASSINGSGEBIED EN INTERPRETATIE | 3 |
| 2.1. | TOEPASSINGSGEBIED VAN DE NORMEN | 3 |
| 2.2. | INTERPRETATIE VAN DE NORMEN | 4 |
| 3. | BEOOGDE DOELSTELLINGEN | 4 |
| 4. | MINIMALE NORMEN – STRUCTUUR ISO 27002:2007 | 4 |
| 5. | BELEID VOOR INFORMATIEVEILIGHEID | 5 |
| 6. | ORGANISATIE VAN DE INFORMATIEVEILIGHEID | 6 |
| 7. | BEHEER VAN BEDRIJFSMIDDELEN | 7 |
| 8. | MEDEWERKERS-GERELATEERDE VEILIGHEID | 8 |
| 9. | FYSIEKE BEVEILIGING EN BEVEILIGING VAN DE OMGEVING | 8 |
| 10. | OPERATIONEEL BEHEER | 9 |
| 11. | TOEGANGSBEVEILIGING (LOGISCH) | 11 |
| 12. | ONTWIKKELING EN ONDERHOUD VAN SYSTEMEN | 12 |
| 13. | BEHEER VAN INCIDENTEN IN VERBAND MET INFORMATIEVEILIGHEID | 13 |
| 14. | CONTINUÏTEITSBEHEER | 13 |
| 15. | NALEVING | 13 |
| 16. | HANDHAVING, OPVOLGING EN HERZIENING | 14 |
| 17. | SANCTIE | 14 |

1. Voorbeschouwing

Het document "Richtlijnen inzake veiligheid op het niveau van de instellingen die deel uitmaken van het netwerk dat wordt beheerd door de Kruispuntbank van de Sociale Zekerheid" legt de door iedere instelling na te streven veiligheidsdoeleinden vast.

De in dit document beschreven minimale veiligheidsnormen daarentegen zijn door de socialezekerheidsinstellingen verplicht na te leven indien zij een toegang willen bekomen en behouden tot het netwerk van de Kruispuntbank. De normen hebben dus een bindende waarde. De controle op de naleving ervan geschiedt door het invullen van een vragenlijst die via de Kruispuntbank ter evaluatie aan het sectoraal comité van de sociale zekerheid en van de gezondheid wordt overgemaakt. Het behoort tot de verantwoordelijkheid van de instelling de vragenlijst correct in te vullen en over de naleving van de normen te waken. Het sectoraal comité van de sociale zekerheid en van de gezondheid kan desgevallend controles ter plaatse (laten) uitvoeren teneinde op het terrein te peilen naar de naleving van de minimale veiligheidsnormen door de socialezekerheidsinstellingen.

Sommige instellingen zijn gehuisvest in verschillende gebouwen of beschikken over (kleine) regionale bureaus. Ook daar moeten de minimale veiligheidsnormen nageleefd worden, in het bijzonder op het vlak van de fysieke beveiliging (toegangsbeveiliging, brandveiligheid, ...).

2. Toepassingsgebied en interpretatie

2.1. Toepassingsgebied van de normen

De hierna toegelichte minimale veiligheidsnormen gelden voor de instellingen van sociale zekerheid, zoals vermeld in artikel 2, eerste lid, 2° van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid¹.

De implementatie en de verificatie van de minimale veiligheidsnormen bij derden die voor rekening van een socialezekerheidsinstelling sociale gegevens van persoonlijke aard verwerken² behoren in eerste instantie tot de verantwoordelijkheid van de instelling die aan de derde werkzaamheden toevertrouwt.

Op basis van de vragenlijsten die door de instellingen ingevuld teruggestuurd worden, kan het sectoraal comité van de sociale zekerheid en van de gezondheid in deze instellingen controles laten uitvoeren door een externe instantie met betrekking tot de naleving van specifieke aspecten van de minimale veiligheidsnormen.

Verder zijn de normen in beginsel enkel van kracht op de verwerking van sociale gegevens van persoonlijke aard. De minimale normen moeten echter ook worden toegepast in het kader van beraadslaging nr. 21/2004 van 12 juli 2004, waarbij een aantal instellingen van sociale zekerheid door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer werden gemachtigd om onder bepaalde voorwaarden toegang te hebben tot het Rijksregister en om het identificatienummer van het Rijksregister te gebruiken voor het verrichten van hun taken inzake personeelsbeheer.

Tot slot dient er te worden opgemerkt dat deze minimumnormen voor herziening vatbaar zijn. Ze zullen aldus worden aangepast in functie van de evolutie die zich op wettelijk, technisch of ander vlak voordoet.

1 en gecoördineerde versie van deze wet is beschikbaar op de website van de Kruispuntbank van de Sociale Zekerheid (http://www.ksz.fgov.be/nl/Legislation/legislat_1.htm).

2 Onder "verwerken" wordt verstaan elke bewerking of geheel van bewerkingen m.b.t. persoonsgegevens, al dan niet met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van verzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen.

Om deze doelstelling te realiseren, zal de werkgroep “Informatieveiligheid” van het Algemeen Coördinatiecomité regelmatig de minimale veiligheidsnormen evalueren en eventueel bijwerken. Indien sommige minimumnormen aangepast moeten worden of minimumnormen toegevoegd moeten worden, zal de werkgroep “Informatieveiligheid” een voorstel voorleggen.

De instellingen die tot het netwerk van de Kruispuntbank wensen toe te treden, moeten over een geactualiseerd meerjarenplan beschikken waarin de maatregelen worden vermeld om aan de normen te voldoen. Het sectoraal comité van de sociale zekerheid en van de gezondheid kan hiervan een kopie opvragen.

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.

3. Beoogde doelstellingen

De minimale veiligheidsnormen beogen:

- de naleving van de toepasselijke wettelijke en reglementaire verplichtingen, voorzien in de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid en haar uitvoeringsbesluiten (onder meer het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid) – de gecoördineerde teksten van deze uitvoeringsbesluiten zijn beschikbaar op de website van de Kruispuntbank van de Sociale Zekerheid.
- de machtiging van de socialezekerheidsinstelling of meewerkende instelling tot deelname aan het netwerk van de Kruispuntbank.

4. Minimale normen – structuur ISO 27002:2007

In de volgende paragrafen worden de minimumnormen gedefinieerd volgens de structuur en de nummering van de ISO-27002-norm.

5. Beleid voor informatieveiligheid

| | Onderwerp | Minimumnorm |
|-----|--|--|
| 5.1 | Information Security Policy ³ . | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• over een formeel, geactualiseerd en door de Directie goedgekeurd beleid voor informatieveiligheid beschikken. |

3 Deze Information Security Policy (ISP) kadert in een beheerssysteem voor informatieveiligheid: de werkgroep "Informatieveiligheid" heeft het initiatief genomen voor de ontwikkeling van een ISMS (Information Security Management System) gebaseerd op de ISO-27002-norm, teneinde tegemoet te komen aan een behoefte van de instellingen van het netwerk om over een gestructureerd en gemeenschappelijk veiligheidsbeleid te beschikken.

Het ISMS is een geïntegreerd systeem dat moet toelaten een optimale beveiliging van de informatie te bereiken. De concrete maatregelen om een optimale informatieveiligheid te bereiken zijn "beleidsmaatregelen" of "controles".

ISMS wordt beschouwd als de **gemeenschappelijke methodologie** die door de instellingen van het netwerk toegepast moet worden om tot een optimale informatieveiligheid te komen. **Het is de verantwoordelijkheid van de instellingen van sociale zekerheid om het ISMS aan te passen aan hun specifieke situatie en aan de omvang van de te beveiligen werkingmiddelen.**

Voor wat de implementatie ervan betreft, dient de informatieveiligheidsconsulent van iedere instelling een beslissing van zijn hiërarchie te verkrijgen.

Het gemeenschappelijk ISMS werd als volgt goedgekeurd door het Algemeen Coördinatiecomité: "Het betreft een basisdocument voor intern gebruik door de instellingen. Het ISMS, dat gebaseerd is op de ISO-27002-norm, bevat de na te leven krachtlijnen. Tussen de veiligheidsconsulent en het leidend personeel dient een permanent overleg georganiseerd te worden."

6. Organisatie van de informatieveiligheid

| | Onderwerp | Minimumnorm |
|-----|------------------------|--|
| 6.1 | Organisatie veiligheid | <p>Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:</p> <ul style="list-style-type: none">• in haar schoot een informatieveiligheidsdienst inrichten die wordt geleid door een veiligheidsconsulent, of die taak toevertrouwen aan een erkende gespecialiseerde informatieveiligheidsdienst. <p>De informatieveiligheidsdienst heeft een adviserende, stimulerende, documenterende en controlerende opdracht (in de zin van het KB van 1993).</p> <p>Met het oog op de veiligheid van de sociale gegevens die door zijn instelling worden verwerkt en met het oog op de bescherming van de persoonlijke levenssfeer van de personen op wie deze sociale gegevens betrekking hebben, staat de veiligheidsconsulent in voor:</p> <ol style="list-style-type: none">1. het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur;2. het uitvoeren van opdrachten die hem door de persoon belast met het dagelijks bestuur worden toevertrouwd. <ul style="list-style-type: none">• de identiteit van haar veiligheidsconsulent en zijn eventuele adjuncten meedelen aan het sectoraal comité van de sociale zekerheid en van de gezondheid. Voor de instellingen van het secundaire netwerk moet de identiteit meegedeeld worden aan de beheersinstelling.• in het bezit zijn van een veiligheidsplan dat door de verantwoordelijke instantie van de betrokken instelling werd goedgekeurd.• over de nodige werkingskredieten beschikken die door de verantwoordelijke instantie van de betrokken instelling werden goedgekeurd, teneinde te kunnen voorzien in de uitvoering van haar veiligheidsplan en de uitvoering door de veiligheidsdienst van de haar opgedragen taken.• aan de Kruispuntbank het aantal uren meedelen dat ze officieel aan de veiligheidsconsulent en aan zijn eventuele adjuncten heeft toegekend voor de uitvoering van hun taken.• de communicatie van informatie aan de veiligheidsconsulent zodanig organiseren dat hij over de gegevens beschikt voor de uitvoering van de hem toegewezen veiligheidsopdracht en om overleg te organiseren tussen de verschillende betrokken partijen⁴ teneinde op deze manier de veiligheidsconsulent nauwer te betrekken bij de werkzaamheden van de instelling. |

⁴ De partijen waar in deze norm naar wordt verwezen zijn voornamelijk de leden van de informaticadienst (ontwikkeling en productie), de preventie-adviseur, de veiligheidsconsulent en de diensten die de gegevens beheren.

| | Onderwerp | Minimumnorm |
|-----|--|--|
| 6.2 | Beslissingsplatform ⁵ | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> beschikken over een beslissingsplatform voor de validatie en de goedkeuring van de veiligheidsmaatregelen. |
| 6.3 | Secundair netwerk | Elke beheersinstelling van een secundair netwerk is ertoe gehouden om minstens één keer per semester relevante informatie uit te wisselen met haar secundair netwerk door een vergadering van de subwerkgroep "Informatieveiligheid" te organiseren voor de instellingen die deel uitmaken van haar netwerk. |
| 6.4 | Veilig gebruik van de beroepskaart voor geneeskundige verzorging | De betrokken veiligheidsconsulenten waken, binnen de eigen instelling, over het veilige gebruik van de beroepskaart voor geneeskundige verzorging zoals vastgelegd in de artikelen 42 tot en met 50 van het koninklijk besluit van 22 februari 1998 ⁶ . |

7. Beheer van bedrijfsmiddelen

| | Onderwerp | Minimumnorm |
|-----|-------------------------------------|---|
| 7.1 | Bescherming van de bedrijfsmiddelen | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> zich ervan vergewissen dat de dragers van de persoonsgegevens en de informaticasystemen die deze gegevens verwerken in geïdentificeerde en beveiligde lokalen geplaatst worden, overeenkomstig hun indeling. Deze lokalen zijn enkel toegankelijk voor de gemachtigde personen en enkel tijdens de uren die voor hun functie gerechtvaardigd zijn. |
| 7.2 | Inventaris | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> over een permanent bijgewerkte inventaris beschikken van het informaticamateriaal en de software. |

5 Het beslissingsplatform zorgt voor de sturing van het veiligheidsbeleid: herziening van het beleid, bijstelling van de beveiligingsmaatregelen, opstelling van beveiligingsplannen, de vaststelling van verantwoordelijkheden en het toezicht op veranderende bedreigingen en incidenten.

6 Koninklijk besluit van 22 februari 1998 houdende uitvoeringsmaatregelen inzake de sociale identiteitskaart (gepubliceerd in het Belgisch Staatsblad van 13 maart 1998); gewijzigd bij het koninklijk besluit van 8 december 1998 (Belgisch Staatsblad van 24 december 1998), bij het koninklijk besluit van 26 april 1999 (Belgisch Staatsblad van 19 juni 1999), bij het koninklijk besluit van 11 december 2000 (Belgisch Staatsblad van 21 december 2001) en bij het koninklijk besluit van 26 mei 2002 (Belgisch Staatsblad van 3 juli 2002).

8. Medewerkers-gerelateerde veiligheid

| | Onderwerp | Minimumnorm |
|-----|-----------------------------|---|
| 8.1 | Internet en e-mail | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• een gedragscode opstellen en toepassen voor internet- en e-mailgebruik. |
| 8.2 | Omgang met persoonsgegevens | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• de interne en externe medewerkers die betrokken zijn bij de verwerking van persoonsgegevens op de hoogte stellen van de vertrouwelijkheids- en veiligheidsplichten t.a.v. deze gegevens. |

9. Fysieke beveiliging en beveiliging van de omgeving

| | Onderwerp | Minimumnorm |
|-----|-----------------------------|--|
| 9.1 | Fysieke toegangsbeveiliging | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten zowel tijdens als buiten de werkuren. |
| 9.2 | Brand, inbraak, water | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade. |
| 9.3 | Stroomvoorziening | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• over een alternatieve stroomvoorziening beschikken om de verwachte dienstverlening te waarborgen. |

10. Operationeel beheer

| | Onderwerp | Minimumnorm |
|------|--|--|
| 10.1 | Toegang tot informaticasystemen door informatiebeheerders ⁷ | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> de toegang van informatiebeheerders tot informaticasystemen beperken door identificatie, authenticatie, en autorisatie. |
| 10.2 | Detectie veiligheidsinbreuken | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> een systeem en formele, geactualiseerde procedures installeren die toelaten om veiligheidsinbreuken te detecteren, op te volgen en te herstellen in verhouding tot het technisch/operationeel risico. |
| 10.3 | Externe TCP/IP-verbinding – primair netwerk | De socialezekerheidsinstellingen van het primaire net moeten: <ul style="list-style-type: none"> voor hun aan de sociale zekerheid externe TCP/IP-verbindingen gebruik maken van het Extranet van de sociale zekerheid⁸. Voor iedere afwijking op deze maatregel moet een gemotiveerde aanvraag via de veiligheidsdienst van de KSZ worden ingediend . |
| 10.4 | Externe TCP/IP-verbinding – secundair netwerk | De socialezekerheidsinstellingen van het secundaire netwerk kunnen voor hun aan de sociale zekerheid externe TCP/IP-verbindingen gebruik maken van het Extranet van de sociale zekerheid ⁹ . Voor de rechtstreekse verbindingen met hun aan de sociale zekerheid externe TCP/IP-netwerken moeten: <ul style="list-style-type: none"> 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; de desbetreffende beheersinstellingen veiligheidsvoorzieningen treffen die in overeenstemming zijn en blijven met de getroffen voorzieningen op het niveau van het Extranet van de sociale zekerheid. |
| 10.5 | Bescherming tegen malware ¹⁰ . | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> over geactualiseerde systemen beschikken ter bescherming |

7 De informatiebeheerder is eenieder die in het kader van zijn verantwoordelijkheden met betrekking tot een ICT-systeem over toegangsrechten beschikt die ruimer zijn dan het louter functionele gebruik van de gegevens. Het gaat onder meer om ontwikkelaars, systeembeheerders, gegevensbeheerders, software-ontwikkelaars en –beheerders, netwerkbeheerders, consultants en onderaannemers.

8 Deze maatregel vervalt indien de betrokken instelling voor haar aan de sociale zekerheid externe TCP/IP-verbindingen gebruik maakt van een computerconfiguratie die niet gebruikt wordt voor de verwerking van sociale gegevens van persoonlijke aard of die in generlei mate verbonden is met het (de) informatiesyste(e)m(en) aangewend voor de verwerking van sociale gegevens van persoonlijke aard.



9 Deze maatregel vervalt indien de betrokken instelling voor haar aan de sociale zekerheid externe TCP/IP-verbindingen gebruik maakt van een computerconfiguratie die niet gebruikt wordt voor de verwerking van sociale persoonsgegevens of die in generlei mate verbonden is met het (de) informatiesyste(e)m(en) aangewend voor de verwerking van sociale persoonsgegevens.

10 Malware : vb. virus, worm, Trojaans paard, spam, spyware

Minimale Normen
(Information Security Management System)

Version 3.13

15/12/2010

| | Onderwerp | Minimumnorm |
|---|---|--|
| | | (voorkoming, detectie en herstel) tegen malware. |
| 10.6 | Nagaan van veiligheidsvereisten vóór inproductiename | <p>Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:</p> <ul style="list-style-type: none"> nazien dat, vooraleer nieuwe of belangrijke evoluties van bestaande systemen in productie genomen worden, de projectverantwoordelijke nagaat of aan de veiligheidsvereisten voldaan werd die aan het begin van de ontwikkelingsfase vastgesteld werden (zie deel "Ontwikkeling"). |
| 10.7  | Veiligheid op netwerkniveau | <p>Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet:</p> <ul style="list-style-type: none"> nazien dat de netwerken gepast beheerd en gecontroleerd worden zodanig dat ze beveiligd zijn tegen bedreigingen en de beveiliging afdoende garanderen van de systemen en toepassingen die het netwerk gebruiken, de noodzakelijke, afdoende, gepaste en doeltreffende technische maatregelen implementeren om het hoogste niveau van beschikbaarheid voor de verbinding met het netwerk van de Kruispuntbank te waarborgen teneinde een maximale toegankelijkheid van de beschikbaar gestelde en geraadpleegde gegevens te verzekeren.. <p>Bijgevolg veronderstelt dit dat deze verbinding minstens ontdubbeld moet zijn naar verschillende knooppunten van het extranet, die de informatie-overdracht ondersteunen en de veiligheidsaspecten integreren ...</p> |
| 10.8 | Informatie-uitwisseling | |
| 10.8.a | Beheer van extranetfluxen | <p>Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet</p> <ul style="list-style-type: none"> de lijst van de openstaande stromen op het extranet van de sociale zekerheid up-to-date houden. |
| 10.8.b  | Kwaliteit van dienstverlening met betrekking tot de uitwisseling van sociale persoonsgegevens | <p>Elke overdracht van sociale gegevens binnen het netwerk van de sociale zekerheid moet zo spoedig mogelijk worden verwerkt door alle betrokken partijen, of ze nu tussenpersoon of bestemming/ontvanger zijn.</p> <p>Instellingen die sociale gegevens versturen binnen het netwerk van de sociale zekerheid, in het bijzonder wanneer ze de authentieke bron zijn, moeten te gepasten tijde de opvolgingsberichten verwerken die ze van de bestemmingen of tussenpersonen moeten ontvangen.</p> <p>Elke bij de verzending betrokken partij, zowel de bestemming/ontvanger als de tussenpersoon of de verzender, moet zo snel mogelijk de gepaste maatregelen nemen bij de verwerking van de opvolgingsberichten.</p> <p>Elke anomalie of lacune in de elektronische verzending van de gegevens moet zo spoedig mogelijk worden gemeld aan de betrokken partijen, of ze nu ontvanger, tussenpersoon of verzender zijn.</p> |

| | Onderwerp | Minimumnorm |
|-------|-----------------------------------|---|
| 10.9 | Back-up-policy procedures en | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> • een systeem van regelmatig te controleren veiligheidskopieën (back-up) invoeren om, in geval van beperkte of totale ramp, 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 besturingsysteem). |
| 10.10 | Logging toegang | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> • een loggingsysteem implementeren voor de persoonsgegevens nodig voor de toepassing en uitvoering van de sociale zekerheid. |
| 10.11 | Zone "USERID" | 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 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 verstuurt. In dat geval moet de instelling van sociale zekerheid 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. |
| 10.12 | Vermijden single point of control | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet over procedures beschikken: <ul style="list-style-type: none"> • 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. |

11. Toegangsbeveiliging (logisch)

| | Onderwerp | Minimumnorm |
|------|----------------------|--|
| 11.1 | Beveiliging gegevens | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> • de toegang tot de gegevens¹¹ nodig voor de toepassing en de uitvoering van de sociale zekerheid beveiligen door middel van een identificatie-, authenticatie- en autorisatiesysteem. |

11 In deze norm wordt onder de term "gegeven" niet enkel de sociale persoonsgegevens verstaan maar alle logische elementen van een informatiesysteem die voor de verwerking ervan instaan. Voorbeelden zijn: programma's, toepassingen, bestanden, systeemutility's en andere elementen van het besturingsysteem.

| | Onderwerp | Minimumnorm |
|------|---|--|
| 11.2 | Toelatingen sectoraal comité | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: zich vergewissen van het bestaan van de noodzakelijke machtigingen van het sectoraal comité voor de toegang tot sociale gegevens van persoonlijke aard beheerd door een andere instelling. |
| 11.3 | Toegang op afstand | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> de gepaste maatregelen treffen, in functie van het toegangsmedium¹², voor de beveiliging van de online-toegang van buiten de instelling tot de persoonsgegevens van de instelling. |
| 11.4 | Bescherming van gegevens op mobiele media ¹³ | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> de gepaste maatregelen nemen indien persoonsgegevens worden opgeslagen op mobiele media die de beveiligingsperimeter van de instelling kunnen verlaten. |

12. Ontwikkeling en onderhoud van systemen

| | Onderwerp | Minimumnorm |
|------|---|--|
| 12.1 | Informatieveiligheid in het kader van projecten | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> over procedures beschikken voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen zodat door de projectverantwoordelijke rekening wordt gehouden met de veiligheidsvereisten die in dit document beschreven worden. |
| 12.2 | Documentatie | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> over procedures beschikken voor de uitwerking van documentatie bij de ontwikkeling van nieuwe en het onderhoud van bestaande toepassingen en systemen. |
| 12.3 | Gestructureerde ontwikkelingsaanpak | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none"> een gestructureerde aanpak gebruiken om de veilige ontwikkeling van systemen na te streven. |

12 Toegangsmedium : vb. internet, gehuurde verbinding, privaat netwerk, draadloos.

13 Mobiele media: verwijderbaar flashgeheugen, draagbare harddisk, laptop, PDA, ...

13. Beheer van incidenten in verband met informatieveiligheid

| | Onderwerp | Minimumnorm |
|------|--------------------------------------|---|
| 13.1 | Belangrijke incidenten ¹⁴ | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• ervoor zorgen dat de dienst Informatieveiligheid door de verantwoordelijke dienst op de hoogte gesteld wordt van belangrijke incidenten die de informatieveiligheid in het gedrang kunnen brengen alsook van de maatregelen die genomen worden om aan deze incidenten het hoofd te bieden. |

14. Continuïteitsbeheer

| | Onderwerp | Minimumnorm |
|------|----------------|---|
| 14.1 | Risico-analyse | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• een continuïteitsplan uitwerken, testen en onderhouden. Dit continuïteitsplan moet gebaseerd zijn op een risico-analyse om de opdracht van de instelling in het kader van de sociale zekerheid te kunnen waarborgen.• een informatica-uitwijkcentrum voorzien in geval van beperkte of totale ramp. |

15. Naleving

| | Onderwerp | Minimumnorm |
|------|-----------------------------|---|
| 15.1 | Externe audit ¹⁵ | Elke socialezekerheidsinstelling aangesloten op het netwerk van de Kruispuntbank moet: <ul style="list-style-type: none">• tenminste één keer om de vier jaar een externe audit organiseren met betrekking tot de situatie van de logische en fysieke veiligheid. |

14 Voorbeelden van belangrijke incidenten: brand, waterschade, malware-aanvallen, intrusie pogingen (fysiek of logisch), diefstal of verlies van draagbare computers, loggingonderbreking, ...

15 Het betreft een audit waarbij het initiatief en de hieraan verbonden financiële inspanningen uitgaan van de instelling zelf. De audit hoeft niet allesomvattend te zijn.

16. Handhaving, opvolging en herziening

De wijziging van de minimale normen geeft aanleiding tot

- de voorlegging van het voorstel tot wijziging van de minimale veiligheidsnormen aan het Beheerscomité van de Kruispuntbank;
- de voorlegging van de gewijzigde vragenlijst aan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid afdeling Sociale Zekerheid;
- het opsturen van de gewijzigde en goedgekeurde minimale veiligheidsnormen naar de verantwoordelijken voor het dagelijks bestuur van de instellingen van sociale zekerheid die hun beheerscomité ervan op de hoogte brengen;
- de nieuw-toegevoegde minimale normen treden in werking één jaar na de goedkeuring door het Beheerscomité van de Kruispuntbank, in casu 1 januari 2011, het gaat over volgende minimale normen:

6.2, 10.7, 10.8.b

Jaarlijks zal een vragenlijst opgestuurd worden naar de sociale instellingen teneinde de naleving van de minimale veiligheidsnormen te evalueren.

De onderwerpen van specifieke veiligheidsmaatregelen die goedgekeurd werden op het niveau van het Algemeen Coördinatiecomité en die nog niet opgenomen werden in een herziene versie van de minimale normen, zullen proactief opgenomen worden in de jaarlijkse vragenlijst.

17. Sanctie

Indien het sectoraal comité van de sociale zekerheid en van de gezondheid vaststelt dat een socialezekerheidsinstelling tekortschiet wat de naleving van deze normen betreft, kan het comité de Kruispuntbank verzoeken om geen gevolg meer te verlenen aan de door die instelling verstuurdde voorleggingen.

Het spreekt echter vanzelf dat, alvorens die maatregel kan worden genomen, het sectoraal comité van de sociale zekerheid en van de gezondheid de persoon ondervraagt die belast is met het dagelijks bestuur van de betrokken instelling.