Minimale normen informatieveiligheid en privacy

(MNM)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

De organisatie van het beleid informatieveiligheid en privacy binnen het netwerk van de Kruispuntbank van de Sociale Zekerheid is gebaseerd op de verplichte toepassing van de minimale normen voor informatieveiligheid en privacy door haar partners, zoals bepaald in het koninklijk besluit van 12 augustus 1993 *houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid*.

De minimale normen informatieveiligheid en privacy scheppen de nodige voorwaarden voor een betrouwbare uitvoering van informatieverwerking voor de openbare instellingen van sociale zekerheid (OISZ) die op het netwerk van de Kruispuntbank van de Sociale Zekerheid aangesloten zijn.

Het is voor de partners binnen de sociale zekerheid belangrijk om deze minimale normen informatieveiligheid en privacy te kennen, te valideren, te communiceren en te integreren.

Dit document beschrijft de minimale normen voor informatieveiligheid en privacy.

2. Toepassingsgebied minimale normen

De toepassing van de minimale normen informatieveiligheid en privacy is verplicht voor instellingen van sociale zekerheid overeenkomstig artikel 2, eerste lid, 2° van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid (KSZ). Bovendien moeten de minimale normen informatieveiligheid en privacy eveneens toegepast worden door alle organisaties die deel uitmaken van het netwerk van de sociale zekerheid overeenkomstig artikel 18 van deze wet. Tenslotte kan het sectoraal comité van de sociale zekerheid en van de gezondheid de naleving van de minimale normen informatieveiligheid en privacy ook opleggen aan andere instanties dan de hogervermelde.

De in dit document beschreven minimale normen zijn verplicht na te leven door de organisaties indien zij een toegang willen bekomen en behouden tot het netwerk van de Kruispuntbank van de Sociale Zekerheid. Deze minimale normen hebben dus een bindende waarde.

Sommige organisaties zijn gehuisvest in verschillende gebouwen of beschikken over (kleine) regionale bureaus. Ook daar moeten de minimale normen informatieveiligheid en privacy nageleefd worden.

Verder zijn de normen in beginsel enkel van kracht op de verwerking van sociale gegevens van persoonlijke aard. De minimale normen informatieveiligheid en privacy 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.

Daarnaast is het nuttig om deze normen ook toe te passen op informatieveiligheid en privacy in de ruime betekenis zoals gedefinieerd in het koninklijk besluit van 17 maart 2013 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, en zoals overgenomen in het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid: ”Strategie, regels, procedures en middelen voor het beschermen van alle soorten informatie zowel in de transmissiesystemen als in de verwerkingssystemen om de vertrouwelijkheid de beschikbaarheid, de integriteit, de betrouwbaarheid, de authenticiteit en de onweerlegbaarheid ervan te garanderen”.

Tenslotte heeft de Europese verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens van 27 april 2016[1] een belangrijke impact op informatieveiligheid en privacy van alle openbare instellingen van sociale zekerheid.

3. Doelstellingen

Deze minimale normen informatieveiligheid en privacy beogen:

A. de naleving van de toepasselijke wettelijke en reglementaire verplichtingen te verzekeren;

B. het vertrouwen van de burgers rond informatie uitwisseling met de overheid te behouden;

C. op een gecoördineerde manier een gepast niveau van informatieveiligheid en privacy te verzekeren;

D. het bekomen of behouden van een machtiging tot uitwisseling van gegevens binnen het netwerk van de Kruispuntbank van Sociale Zekerheid (KSZ).

4. Wat en waarom?

4.1 Wat is informatieveiligheid?

Informatie is een essentieel middel dat adequate bescherming vereist. In de snel evoluerende wereld van vandaag wordt informatie meer dan ooit blootgesteld aan allerlei bedreigingen en kwetsbaarheden.

Informatie, in welke vorm ook (geschreven, gesproken, afgedrukt, opgeslagen, verstuurd per post of elektronisch), moet gepast beschermd worden tegen externe en interne bedreigingen en kwetsbaarheden. Elke directie en elke verwerker van informatie heeft de verantwoordelijkheid om de continuïteit van informatieverwerking te verzekeren en om de vertrouwelijkheid en de integriteit van de informatie te beheren.

Elke organisatie streeft informatieveiligheid na via effectieve en efficiënte controlemaatregelen. Deze controlemaatregelen worden dynamisch beheerd en continu geoptimaliseerd waar nodig, om zo de doelstelling van de organisatie te realiseren. Elke organisatie integreert informatieveiligheid zo veel mogelijk direct in alle processen.

4.2 Wat is privacy?

Elk individu heeft recht op bescherming van zijn of haar persoonsgegevens: “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon”[2].

Daarnaast heeft elk individu recht op bescherming van de verwerking van zijn of haar persoonsgegevens: “een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens”.

Elke organisatie streeft privacybescherming na via effectieve en efficiënte controlemaatregelen. Deze controlemaatregelen worden dynamisch beheerd en continu geoptimaliseerd waar nodig, om zo de doelstelling van de organisatie te realiseren. Elke organisatie integreert privacybescherming zo veel mogelijk direct in alle processen.

[1] EU GDPR http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] Definitie van persoonsgegevens zoals vermeld in de EU GDPR http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

4.3 Waarom zijn informatieveiligheid en privacy essentieel?

Informatie en de daarbij horende processen, systemen en netwerken zijn belangrijke middelen voor een organisatie. Het definiëren, implementeren, onderhouden en verbeteren van informatieveiligheid en privacy is essentieel om het vertrouwen van de burgers te behouden, om de wettelijke verplichtingen na te (blijven) komen en om de reputatie van de organisatie te vrijwaren.

De technologische maatregelen zijn niet allesomvattend en moeten steeds aangevuld worden met de gepaste organisatorische, procedurele en communicatieve elementen die gebaseerd zijn op een risico-beoordeling of op wettelijke en regelgevende verplichtingen.

Het beheren van informatieveiligheid en privacy vereist de actieve deelname van alle medewerkers, burgers, organisaties, leveranciers en andere externe partijen. Immers, een organisatie –met inbegrip van de informatie en informatiesystemen- krijgt te maken met diverse bedreigingen en problemen. Deze bedreigingen en problemen komen steeds vaker voor. Het aanvallen van informatiesystemen is relatief eenvoudig en goedkoop op te zetten. De aanvallen worden steeds gesofisticeerder. De problemen worden steeds complexer. De gepaste controlemaatregelen om hieraan weerstand te bieden (voorkomen én herstellen) vereisen inzicht, planning en voldoende middelen.

5. Minimale Normen

Elke organisatie onderschrijft de volgende minimale normen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

5.1. Kernprincipes

	Onderwerp	Minimumnorm
5.1.1	Kernprincipes	Elke organisatie moet de kernprincipes opnemen in haar informatieveiligheidsbeleid.

5.2. Beleid voor informatieveiligheid

	Onderwerp	Minimumnorm
5.2.1	Information Security Policy[3].	Elke organisatie moet over een formeel, geactualiseerd en door de verantwoordelijke voor het dagelijkse bestuur (of gelijkwaardig), goedgekeurd beleid voor informatieveiligheid beschikken.
5.2.2	Risico-beoordeling	Elke organisatie moet : a. bij elk proces en bij elk project een risico-beoordeling rond informatieveiligheid en privacy uitvoeren, valideren, communiceren en

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 (**I**nformation **S**ecurity **M**anagement **S**ystem) geïnspireerd op de ISO-27001-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 werkingsmiddelen.**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."

		onderhouden b. alle risico-beoordelingen met een hoog residueel risico communiceren naar de directie voor bespreking en beslissing : behandelen of aanvaarden. c. de richtlijn rond risico-beoordeling toepassen zoals vermeld in bijlage C van de beleidslijn 'Risico-beoordeling'.

5.3. Organisatie van de informatieveiligheid

5.3.1. Interne organisatie

	Onderwerp	Minimumnorm
5.3.1.1	Personeelsgerelateerde aspecten	Elke organisatie moet Voorafgaand aan het dienstverband: • De achtergrond nagaan van kandidaten voor functies die een belangrijk risico vormen voor informatieveiligheid. Deze verificatie moet uitgevoerd worden overeenkomstig relevante wetten en voorschriften, en moet evenredig zijn met de eisen, de classificatie van de informatie waartoe toegang verleend wordt, en de ingeschatte risico's. • Als onderdeel van hun contractuele verplichting dienen ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en hun arbeidscontract te ondertekenen, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatieveiligheid en privacy moeten vastgelegd zijn. Tijdens het dienstverband: • De directie moet van werknemers, ingehuurd personeel en externe gebruikers eisen dat ze informatieveiligheid en privacy toepassen overeenkomstig de minimale normen en procedures van de organisatie • Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, moeten geschikte training en regelmatige bijscholing krijgen met betrekking tot minimale normen en procedures van de organisatie, voor zover relevant voor hun rol of functie • Regelmatig actualiseren van de verificatie van de achtergrond van medewerkers voor functies die een belangrijk risico vormen voor informatieveiligheid en privacy, overeenkomstig relevante wetten en voorschriften. Deze verificatie moet evenredig zijn met de vereisten, de classificatie van de informatie waartoe toegang verleend wordt, en de ingeschatte risico's • Er moet een formeel disciplinair proces voorzien zijn voor medewerkers die een inbreuk op informatieveiligheid of privacy hebben gepleegd, en dit in overeenstemming met sancties voor niet naleving zoals voorzien in de wetgeving Beëindiging of wijziging van dienstverband: • De verantwoordelijkheden en verplichtingen rond informatieveiligheid en privacy die geldig blijven na beëindiging of wijziging van het dienstverband moeten duidelijk zijn vastgesteld, gecommuniceerd worden aan de medewerker, ingehuurd personeel en externe gebruikers, en afgedwongen worden.

	Onderwerp	Minimumnorm
5.3.1.2	Organisatie van informatieveiligheid	Elke organisatie moet: a. een informatieveiligheidsdienst inrichten die wordt geleid door een veiligheidsconsulent, of die taak toevertrouwen aan een erkende gespecialiseerde informatieveiligheidsdienst. b. de identiteit van haar veiligheidsconsulent en zijn eventuele adjuncten meedelen aan het sectoraal comité van de sociale zekerheid en van de gezondheid. Voor de organisaties van het secundaire netwerk moet de identiteit meegedeeld worden aan de verantwoordelijke instelling voor dit netwerk. c. in het bezit zijn van een veiligheidsplan dat door de verantwoordelijke voor het dagelijkse bestuur van de betrokken organisatie (of gelijkwaardig),werd goedgekeurd. d. over de nodige werkingskredieten beschikken die door de verantwoordelijke voor het dagelijkse bestuur van de betrokken organisatie (of gelijkwaardig) werden goedgekeurd, teneinde te kunnen voorzien in de uitvoering van haar veiligheidsplan en de uitvoering door de veiligheidsdienst van de haar opgedragen taken. e. aan de KSZ het aantal uren meedelen dat ze officieel aan de veiligheidsconsulent en aan zijn eventuele adjuncten heeft toegekend voor de uitvoering van hun taken. f. een periodieke communicatie van informatie aan de veiligheidsconsulent organiseren zodat hij over de gegevens beschikt voor de uitvoering van de hem toegewezen veiligheidsopdracht en om overleg te organiseren tussen de verschillende betrokken partijen[4] teneinde op deze manier de veiligheidsconsulent nauwer te betrekken bij de werkzaamheden van de organisatie.
5.3.1.3	Beslissingsplatform[5]	Elke organisatie moet beschikken over een beslissingsplatform voor de validatie en de goedkeuring van de informatieveiligheid- en privacy-maatregelen
5.3.1.4	Secundair netwerk	Elke organisatie van een secundair netwerk moet minstens één keer per semester relevante informatie uitwisselen met haar secundair netwerk door een vergadering van de subwerkgroep "Informatieveiligheid" te organiseren voor de organisaties die deel uitmaken van haar netwerk
5.3.1.5	Informatieveiligheid in het kader van projecten	Elke organisatie moet over procedures beschikken voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen zodat door de projectverantwoordelijke rekening wordt gehouden met de informatieveiligheid- en privacy-vereisten die in dit document beschreven worden

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.

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.

5.3.2. Mobiele apparatuur en telewerken

	Onderwerp	Minimumnorm
5.3.2.1	Veilig gebruik van mobiele toestellen	Elke organisatie moet a. de gepaste maatregelen nemen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen. b. de gepaste maatregelen treffen, in functie van het toegangsmedium[6], voor de informatieveiligheid van de toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie. c. de voorwaarden opleggen, die gedetailleerd zijn in de beleidslijn ' mobiele toestellen', bij het gebruik van privé-toestellen voor beroepsdoeleinden. d. de regels opleggen , die gedetailleerd zijn in de beleidslijn ' mobiele toestellen', bij het gebruik van de mobiele toestellen voor zowel beroepsdoeleinden als voor privé-doeleinden. e. de eigen mobiele toestellen duidelijk identificeren, veilig configureren (met de nodige anti-malware software en met software die alle data op het toestel vanop afstand kunnen wissen) en de identificatie bijhouden in een centraal register. f. gepaste controles implementeren[7] om de conformiteit van de mobiele toestellen inzake de beleidslijnen informatieveiligheid en privacy controleren (vanop afstand via software of ter plaatse via directe controle). De organisatie is niet verantwoordelijk voor schade of kosten als gevolg van het verlies of de diefstal van privé gegevens. g. de gebruikers regelmatig sensibiliseren omtrent de goede praktijken inzake gebruik en hun verantwoordelijkheden (zeker in verband met het connecteren tot publieke draadloze netwerken). h. de mogelijkheid hebben om de toegang tot de informatie van de organisatie (gegevens of toepassingen aanwezig op het mobiele toestel) direct te blokkeren en de gegevens te wissen. i. zich ertoe verbinden om de privacy van de gebruiker te respecteren.
5.3.2.2	Veilig telewerken	Elke organisatie moet a. de gepaste maatregelen treffen, in functie van het toegangsmedium[8], voor de informatieveiligheid van de toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie b. duidelijk gedragsregels en een gepaste implementatie van telewerken opzetten, valideren, communiceren en onderhouden, inclusief de uitwerking van welke systemen niet, en welke systemen wel vanuit de thuiswerkplek of andere apparaten mogen worden geraadpleegd. c. de telewerk-voorzieningen van de organisatie zo inrichten dat er op de telewerk-plek (thuis, in een satellietkantoor of in een andere locatie) geen

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

7 Steeds op basis van een wederzijds akkoord tussen de organisatie en de gebruiker.

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

	Onderwerp	Minimumnorm
		informatie van de organisatie wordt opgeslagen op externe toestellen zonder versleuteling en dat mogelijke bedreigingen vanaf de telewerk-plek niet in de IT infrastructuur van de organisatie terechtkomen.

5.4. Medewerkers-gerelateerde veiligheid (Clean desk & Clear desk)

	Onderwerp	Minimumnorm
5.4.1	Rapportering, evaluatie en sensibiliserings-campagne	Elke organisatie moet • minstens jaarlijks een sensibiliseringscampagne of informatiesessie met betrekking tot informatieveiligheid en privacy opzetten, valideren, communiceren en opvolgen. • jaarlijks een evaluatie uitvoeren rond de naleving van dit beleid in de praktijk (via interne enquête).
5.4.2	Toegang tot de informatie	Elke organisatie moet a. Een beleidslijn uitwerken waarbij wordt aangegeven dat de medewerking van alle medewerkers van essentieel belang is voor de informatieveiligheid en de privacy. Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen of tot documenten. b. Een beleidslijn uitwerken waarbij wordt aangegeven dat de gebruiker steeds verantwoordelijk blijft voor de informatie, ongeacht de vorm waarin deze informatie wordt opgeslagen. De gebruiker moet dus zorgen voor een goede bescherming ervan. Zodra de informatie niet meer wordt gebruikt door de gebruiker, moet de gebruiker zorgen voor de archivering of verwijdering ervan. d. Een (logisch of fysiek) toegangssysteem implementeren om elke ongeoorloofde toegang tot de organisatie te voorkomen. De toegang wordt beveiligd door een duidelijke toegangsprocedure.

5.5. Beheer van bedrijfsmiddelen

	Onderwerp	Minimumnorm
5.5.1	Data classificatie	Elke organisatie moet a. voorziene bescherming of classificatie van informatie toepassen inclusief bijhorende informatieveiligheid- en privacy-maatregelen volgens een intern classificatieschema dat in lijn is met de specifieke wetgeving terzake alsook met de internationale regelgeving[9]. b. gepaste procedures en registers opstellen, valideren, implementeren, communiceren en onderhouden voor het labelen (etiketteren) en voor het verwerken van alle in beheer zijnde informatieverzamelingen, informatiedragers en informatiesystemen in overeenstemming met het interne classificatieschema.

[9] in het bijzonder de wetgeving van 11 december 1998 betreffende de classificatie en veiligheidsmachtigingen

	Onderwerp	Minimumnorm
		c. De regel toepassen dat de classificatie die door de soort informatie bepaald wordt ook geldt voor het hogere niveau van informatiesystemen, dat wil zeggen dat, indien een systeem geheime informatie verwerkt, het hele systeem als geheim wordt aangemerkt, tenzij voor dat hogere niveau maatregelen genomen zijn binnen het informatiesysteem. d. Alle classificaties van alle kritieke systemen moeten centraal vastgelegd worden door de eigenaren. e. Alle classificaties van alle kritische systemen moeten jaarlijks gecontroleerd worden door de informatieveiligheidsconsulent (CISO) en/of de functionaris voor gegevensbescherming (DPO). f. De controlemaatregelen afstemmen op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van de te nemen maatregelen.
5.5.2	Inventaris	Elke organisatie moet over een permanent bijgewerkte inventaris beschikken van het informaticamateriaal en de software.
5.5.3	Bescherming van de bedrijfsmiddelen	Elke organisatie moet zich ervan vergewissen dat de dragers van de persoonsgegevens en de informaticasystemen die deze gegevens verwerken[10] 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.
5.5.4	E-mail, online communicatie en internet gebruik	Elke organisatie moet : a. de regels verwerken in haar beleid voor informatieveiligheid en privacy die gespecifieerd zijn in bijlage C van de beleidslijn 'Email, online communicatie en internet gebruik'. Deze regels zijn beschreven in de paragrafen : • gebruiken van e-mail en online communicatiemiddelen • veilig gebruik van internet b. een permanente controle uitoefenen op het 'Email, online communicatie en internet gebruik' in het kader van de volgende doelstellingen: • de bescherming van de reputatie en de belangen van de organisatie; • het voorkomen van ongeoorloofde handelingen of handelingen die indruisen tegen de goede zeden of die de waardigheid van een persoon kunnen schaden; • de veiligheid en/of de goede technische werking van de netwerksystemen van de organisatie, met inbegrip van de beheersing van de eraan verbonden kosten, alsook de fysieke beveiliging van de installaties van de organisatie; • de naleving van de kernprincipes.
5.5.5	Transport van fysieke media	Elke organisatie moet de nodige maatregelen treffen om fysieke media, bijvoorbeeld backups die gevoelige gegevens bevatten, tijdens het transport te beschermen tegen niet geautoriseerde toegang.

5.6. Toegangsbeveiliging (logisch)

	Onderwerp	Minimumnorm

[10]Onder "verwerken" wordt elke bewerking of geheel van bewerkingen van persoonsgegevens verstaan, al dan niet met behulp van geautomatiseerde procedés, 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.

	Onderwerp	Minimumnorm
5.6.1	Toegangsbeheer van portalen	Iedere organisatie die gebruik wenst te maken van de diensten en toepassingen van het portaal van de sociale zekerheid ten behoeve van zijn gebruikers moet : a. minstens één toegangsbeheerder aanstellen b. zijn medewerkers aanzetten tot het lezen en toepassen van de reglementen over het gebruik van de informatiesystemen van de portalen. c. de verplichtingen naleven die gepaard gaan met het uitoefenen van de functie beheerder of medebeheerder en die beschreven zijn in de beleidslijn 'veilig toegangsbeheer van portalen'
5.6.2	Toegang tot het netwerk KSZ via internet	Elke organisatie moet : • een schriftelijke machtiging en afwijking aanvragen aan de leidende ambtenaar van de KSZ wanneer ze wil gebruik maken van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ). Het gebruik van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ) vormt een uitzondering op het algemene principe van de toegang via het Extranet van de Sociale Zekerheid. • de inhoud van de machtigings- en afwijkingsaanvraag moet voldoen aan de specificaties vermeld in de paragraaf 'inhoud van de aanvraag' van de beleidslijn 'Gebruik van internet om toegang te krijgen tot het netwerk van de Kruispuntbank van de Sociale Zekerheid in het kader van de verwerking van persoonsgegevens door de actoren van de sociale sector' • tevens , wanneer ze wil gebruik van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ) strikt de voorwaarden toepassen die zijn opgesomd in de bijlage D (Voorwaarden voor toegang tot het Extranet van de Sociale Zekerheid via internet) van de beleidslijn. Deze voorwaarden hebben betrekking op : ○ Niveau toegangsmachtiging ○ Niveau identificatie / authenticatie ○ Traceerbaarheid ○ Beperkingen ○ Verbinding via file transfer
5.6.3	Beveiliging gegevens	Elke organisatie moet de toegang tot de gegevens[11] nodig voor de toepassing en de uitvoering van de sociale zekerheid beveiligen door middel van een identificatie-, authenticatie- en autorisatiesysteem.
5.6.4	Toelatingen sectoraal comité	Elke organisatie moet zich vergewissen van het bestaan van de noodzakelijke machtigingen van het bevoegde sectoraal comité voor de toegang tot (sociale) persoonsgegevens beheerd door een andere organisatie.

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 besturingssysteem.

	Onderwerp	Minimumnorm
5.6.5	Toegang tot informaticasystemen door informatiebeheerders [12]	Elke organisatie moet de toegang van informatiebeheerders tot informaticasystemen beperken door identificatie, authenticatie, en autorisatie.
5.6.6	Gebruik van netwerk diensten	Elke organisatie moet de gepaste maatregelen treffen opdat iedere persoon slechts toegang zou hebben tot de diensten waarvoor hij uitdrukkelijk een autorisatie heeft verkregen.
5.6.7	Externe IP-verbinding – primair netwerk	Elke instelling van de sociale zekerheid van het primaire netwerk moet het Extranet van de sociale zekerheid[13] gebruiken voor alle externe verbindingen of de verbindingen met haar secundaire netwerk.[14] Voor iedere afwijking op deze maatregel moet een gemotiveerde aanvraag via de veiligheidsdienst van de KSZ worden ingediend.
5.6.8	Externe IP-verbinding – secundair netwerk	Elke organisatie behorend tot een secundair netwerk kan gebruik maken van het Extranet van de sociale zekerheid voor haar verbindingen extern aan de sociale zekerheid. Indien de organisatie een verbinding heeft met externe netwerken zonder te passeren via het Extranet van de sociale zekerheid moet: • de betrokken organisatie veiligheidsmaatregelen implementeren die een gelijkaardig veiligheidsniveau garanderen als dat van het Extranet van de sociale zekerheid voor de informaticasystemen die gebruikt worden voor de verwerking van de persoonsgegevens; • de beheersinstelling van het secundaire netwerk veiligheidsvoorzieningen treffen die een gelijkaardig veiligheidsniveau garanderen als dat van het Extranet van de sociale zekerheid.

5.7. Vercijferen

	Onderwerp	Minimumnorm
5.7.1	Vercijferen	Elke organisatie moet: • een formeel beleid voor het gebruik van cryptografische controles opzetten, valideren, communiceren en onderhouden. Hierbij moet ze gebruik maken van de 'Richtlijnen rond het gebruik van cryptografische controles' zoals opgesomd in de bijlage C van de beleidslijn 'vercijferen'. • een formeel beleid voor het gebruik, bescherming en levensduur van cryptografische sleutels voor de ganse levenscyclus opzetten, valideren, communiceren en onderhouden. Hierbij moet ze gebruik maken van de 'Richtlijnen rond het sleutel beheer' zoals opgesomd in de bijlage D van de

12 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.

13 Het extranet van de sociale zekerheid is de technische ondersteuning die toelaat om elektronische gegevens uit te wisselen in het kader van het netwerk van de Kruispuntbank van de sociale zekerheid (meer informatie over het Extranet is beschikbaar op de website van de Kruispuntbank van de sociale zekerheid).

14 Deze maatregel vervalt voor de informaticasystemen, die niet gebruikt worden voor de behandeling van sociale persoonsgegevens en die op geen enkele wijze verbonden zijn met informaticasystemen die wel gebruikt worden voor de behandeling sociale persoonsgegevens.

	Onderwerp	Minimumnorm
		beleidslijn 'vercijferen'.

5.8. Fysieke beveiliging en beveiliging van de omgeving

	Onderwerp	Minimumnorm
5.8.1	Beveiligde ruimten	Elke organisatie moet de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten zowel tijdens als buiten de werkuren. a. Er moeten toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) worden aangebracht om ruimten te beschermen waar zich gevoelige of kritieke informatie en ICT voorzieningen bevinden. b. Privaat toegankelijke zones van een gebouw en de beveiligde ruimten moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten c. Er moet fysieke beveiliging van kantoren, ruimten en faciliteiten worden ontworpen en gerealiseerd d. Elke organisatie moet maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade e. Er moeten fysieke bescherming en richtlijnen voor werken in beveiligde ruimten worden ontworpen en gerealiseerd f. Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, moeten worden beheerst en indien mogelijk worden afgeschermd van kritieke en/of ICT voorzieningen, om onbevoegde toegang te voorkomen
5.8.2	Beveiliging van apparatuur	Elke organisatie moet maatregelen treffen ter voorkoming van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten a. Kritieke apparatuur moet zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd. b. Elke organisatie moet over een alternatieve stroomvoorziening beschikken om de verwachte dienstverlening te waarborgen. Kritieke apparatuur moet worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen c. Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, moeten tegen interceptie of beschadiging worden beschermd d. Kritieke apparatuur moet op correcte wijze worden onderhouden, zodat deze voortdurend beschikbaar is en in goede staat verkeert e. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder voorafgaande toestemming van de locatie worden meegenomen f. Apparatuur buiten de locaties moet worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de

	Onderwerp	Minimumnorm
		organisatie g. Elke organisatie moet de nodige maatregelen treffen opdat alle gegevens op opslagmedia gewist of ontoegankelijk gemaakt worden vóór verwijdering of hergebruik. h. Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt.
5.8.3	Wissen van elektronische informatiedragers	Elke organisatie moet : a. bij het gebruik van vercijfering als preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager • De encryptiesleutels nooit aanbrengen in een duidelijke vorm op de drager zelf. • De vercijfering moet betrekking hebben op logische volumes in hun geheel (in plaats van op bestanden of individuele repertoria). • De vercijfering dient als aanvulling op de toepasbare organisatorische en procedurele maatregelen die er op gericht zijn om misbruiken tegen te gaan. b. Bij hergebruik van de informatiedrager deze opnieuw gebruiken in een minstens vergelijkbaar data classificatieniveau. c. een risico-beoordeling uitvoeren om de gepaste methode[15] te bepalen voor het wissen van een informatiedrager. d. Bij een voor de organisatie niet aanvaardbaar residuele risico[16] van het terugvinden van de gegevens na het wissen, de informatiedrager fysiek vernietigen, zelfs als het residuele risico hypothetisch is. e. de gepaste maatregelen voor het wissen van gegevens contractueel vastleggen wanneer : • de organisatie informatiedragers gebruikt die geen eigendom zijn (bijvoorbeeld in het kader van leasing of disaster recovery) • de organisatie de technologie niet beheerst voor toegang tot alle niveaus van de informatiedrager (bijvoorbeeld in het kader van cloud computing).

5.9. Operationeel beheer

	Onderwerp	Minimumnorm
5.9.1	Scheiding van omgevingen	Elke organisatie moet zich ervan verzekeren dat er geen testen of ontwikkelingen plaatsvinden in de productieomgeving. In bepaalde uitzonderlijke gevallen kan voor testdoeleinden afgeweken worden van deze regel op voorwaarde dat gepaste maatregelen getroffen worden.
5.9.2	Het beheer van de in productie stelling	Elke organisatie moet: • over procedures beschikken voor het in productie stellen van nieuwe

[15] Zie bijlage D van de beleidslijn 'wissen van elektronische informatiedragers'

[16] de waarschijnlijkheid dat een negatieve impact zich zal voordoen, ondanks de maatregelen die genomen worden om het (inherent) risico te beïnvloeden (beperken)

	Onderwerp	Minimumnorm
		toepassingen en het aanpassen van bestaande toepassingen • voorkomen dat een enkele persoon alleen de controle zou verwerven over dit proces.
5.9.3	Bescherming tegen malware[17].	Elke organisatie moet over geactualiseerde systemen beschikken ter bescherming (voorkoming, detectie en herstel) tegen malware.
5.9.4	Backup-policy	Om onherstelbaar verlies van gegevens te voorkomen, moet elke organisatie: • de policy en strategie definiëren om een backupsysteem te implementeren, in overeenstemming met het continuïteitsbeheer (norm 5.14.). • in dit verband regelmatig de genomen backups verifiëren.
5.9.5	Logging toegang	Elke organisatie moet: • een formele procedure van logbeheer opzetten, valideren, communiceren en onderhouden. • transacties, controlewerkzaamheden, activiteiten van gebruikers, uitzonderingen en informatieveiligheid- en privacy-gebeurtenissen/incidenten gestructureerd vastleggen in afzonderlijke logbestanden, zodat iedere handeling naar de brondocumenten herleid kan worden of de uitgevoerde bewerking(en) gecontroleerd kan(kunnen) worden. • Logbeheer moet meegenomen worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren. • Elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, moet gelogd worden in overeenstemming met de toepasselijke wetgeving en regelgeving. • De interne klokken van alle informatiesystemen van de organisatie moeten gesynchroniseerd worden met een overeengekomen nauwkeurige tijdsbron zodat een betrouwbare analyse van logbestanden op verschillende informatiesystemen altijd mogelijk is. • De noodzakelijke tools moeten beschikbaar zijn of ontwikkeld worden om log gegevens te kunnen laten analyseren door de geautoriseerde personen. • systeemgebruik moet zoveel als mogelijk automatisch worden gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een manueel logboek door systeembeheerders. • Logbestanden moeten beschermd worden tegen inzage door onbevoegden, wijzigingen en verwijderingen. • De logbestanden moeten gedurende een overeengekomen periode worden bewaard, ten behoeve van toekomstig onderzoeken en controles en in overeenstemming met wetgeving en regelgeving[18]. • De raadpleging van logbestanden moet altijd het voorwerp zijn van een

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

18 Zoals de EU GDPR

	Onderwerp	Minimumnorm
		georganiseerde procedure binnen de organisatie met een historiek van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd. • Het resultaat van logbeheer moet regelmatig geanalyseerd, gerapporteerd en beoordeeld worden
5.9.6	Traceerbaarheid van de identiteiten.	Elke organisatie die deelneemt aan het verzenden van gegevens via de Kruispuntbank moet op haar niveau de traceerbaarheid van de identiteiten waarborgen. Deze traceerbaarheid moet identificatie toelaten van begin tot einde[19].
5.9.7	Detectie veiligheidsinbreuken	Elke organisatie moet 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.

5.10. Communicatiebeveiliging

	Onderwerp	Minimumnorm
5.10.1	Veilige draadloze netwerken	Elke organisatie moet voor alle draadloze netwerken onder beheer van de organisatie op alle locaties : a. de draadloze netwerken beheren en beheersen om toegang tot en gebruik van het netwerk te beperken, en om de informatie in systemen en toepassingen te beschermen die over draadloze netwerken wordt verstuurd b. de richtlijnen naleven die beschreven zijn in bijlage C van de beleidslijn 'veilige draadloze netwerken'
5.10.2	Beheer van de veiligheid van het netwerk	Elke organisatie moet 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.
5.10.3	Beschikbaarheid van het netwerk	Elke organisatie moet 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. Bijgevolg veronderstelt dit dat deze verbinding minstens ontdubbeld moet zijn naar verschillende knooppunten van het Extranet.
5.10.4	Cartografie van extranet fluxen	Elke organisatie moet een geactualiseerde cartografie bijhouden van de geïmplementeerde technische[20] stromen via het Extranet van de sociale zekerheid. De veiligheidsconsulent moet hierover geïnformeerd worden
5.10.5	Kwaliteit van dienstverlening met	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

[19] Bijvoorbeeld, 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 verstuurde. 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.

20 Technische stromen op netwerkniveau voor het correct beheer van de firewalls in de verschillende zones van het Extranet.

	Onderwerp	Minimumnorm
	betrekking tot de uitwisseling van sociale persoonsgegevens	tussenpersoon of bestemmeling/ontvanger zijn. 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 bestemmelingen of tussenpersonen moeten ontvangen. Elke bij de verzending betrokken partij, zowel de bestemmeling/ontvanger als de tussenpersoon of de verzender, moet zo snel mogelijk de gepaste maatregelen nemen bij de verwerking van de opvolgingsberichten. 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.

5.11. Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen

	Onderwerp	Minimumnorm
5.11.1	Communicatie	Elke organisatie moet een efficiënte en constructieve communicatie opzetten tussen de verschillende bij het project betrokken partijen (inclusief klanten en leveranciers), in het bijzonder met de veiligheidsconsulent(en). Dit moet een adequaat niveau van informatieveiligheid en privacy garanderen gekend door iedereen
5.11.2	Toegangsbeheer	Elke organisatie moet: a. alle medewerkers laten werken met ICT middelen (die door de instelling ter beschikking worden gesteld) op basis van minimale autorisatie voor de uitvoering van hun taak. b. bij het ontwikkelen van de toegangsbeveiliging rekening houden met de reeds bestaande operationele systemen voor het toegangsbeheer (zoals UAM) en hun evolutie. c. de vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) definiëren, documenteren, valideren en communiceren. Deze toegangen zullen gelogd worden. d. Het beheer van de toegangen, intern in een applicatie, moet zo veel mogelijk vermeden worden. In uitzonderlijk voorkomend geval moeten formele procedures bestaan om alle fases in de levenscyclus van de toegangsbeveiliging te beheren (invoer, controle op basis van een inventaris, mutatie, schrapping). e. Wanneer een programma ontwikkeld wordt waarin de sociale zekerheidsinstelling een programmanummer overneemt in een bericht dat ze aan de KSZ richt, maar een natuurlijk persoon aan de basis van dit bericht ligt, in staat zijn zelf de relatie te leggen tussen dit programmanummer en de identiteit van de natuurlijke persoon die het bericht verstuurt.
5.11.3	Uitbesteding aan derden	Elke organisatie moet de veiligheids- en privacy-risico's contractueel vastleggen en een vertrouwelijkheids- en continuïteitsclausules voorzien.
5.11.4	Checklist	Elke organisatie dient altijd een controlelijst te voorzien voor de projectleider zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en privacy correct geëvalueerd en indien

	Onderwerp	Minimumnorm
		noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project
5.11.5	Controle voor in productie stelling	Elke organisatie moet zich via de verantwoordelijke van de opvolging, de project leider, en bij de in productiestelling van het project er van vergewissen dat de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden.
5.11.6	Gestructureerde aanpak	Elke organisatie moet onder de supervisie van de projectleider de voorzieningen voor ontwikkeling, test en/of acceptatie en productie scheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project.
5.11.7	Logbeheer tijdens een project	Elke organisatie moet: a. Elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, loggen in overeenstemming met de beleidslijnen “logging” en de toepasselijke wetgeving en regelgeving. b. In de specificaties van een project opnemen hoe de toegang tot en het gebruik van systemen en applicaties gelogd zal worden om bij te dragen tot de detectie van afwijkingen van de beleidslijnen informatieveiligheid en privacy. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen : a. Glashelder, snel en eenvoudig kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie b. De identificatie van de aard van de geraadpleegde informatie c. De duidelijke identificatie van de persoon c. rekening houden met reeds bestaande logbeheersystemen bij de evaluatie van logbehoeften in het kader van het project. d. De noodzakelijke tools ter beschikking hebben of ontwikkelen om toe te laten deze log gegevens uit te baten door de geautoriseerde personen. e. De algemene regel toepassen dat de transactionele/functionele log gegevens minimaal 10 jaar en de technische/infrastructurele log gegevens minimaal 2 jaar moeten bewaard blijven.
5.11.8	Back-up/Restore	Elke organisatie moet de deliverables van het project integreren in het backup beheersysteem van de organisatie zoals opgelegd in de beleidslijnen. Dit omvat niet alleen de gegevens die verwerkt worden maar ook de documentatie die hierop betrekking heeft (broncode, programma’s, technische documenten, …). De backup dient regelmatig getest te worden via een herstel (“restore”) oefening om na te gaan of de informatie überhaupt wel recupereerbaar is en hoelang dergelijke herstel opdracht duurt.
5.11.9	Continuïteitsbeheer tijdens een project	Elke organisatie moet: a. In de loop van de ontwikkeling van het project de behoeften met betrekking tot continuïteit van de dienstverlening formaliseren, conform met de verwachtingen van de organisatie. b. In de programma’s de te definiëren herstartpunten duidelijk integreren om het hoofd te bieden aan operationele problemen. Deze informatie maakt deel uit van het exploitatie dossier. c. Tijdens de ontwikkeling van een project bijzondere aandacht besteden aan

	Onderwerp	Minimumnorm
		backup en herstel (“restore”) van informatie d. In de productie omgeving rekening houden met de eisen van de instelling met betrekking tot probleemtolerantie en redundantie van de infrastructuur e. Het continuïteitsplan en de bijhorende procedures actualiseren in functie van de projectevolutie, met inbegrip van continuïteitstesten f. een risico analyse in het begin van het project uitvoeren om de noodprocedures te definiëren. Deze moeten bevatten : • De werking bij verminderde beschikbaarheid van informatie systemen • De beschrijving van alternatieve informatie systemen met inbegrip van de uitrol, de exploitatie modaliteiten en de eventuele ontwikkeling van noodsystemen • De kerntaken en kernprocedures in geval van systeemonderbreking • De taken, de sleutelrollen en de in te zetten middelen om tot een optimale beschikbaarheid te komen.
5.11.10	Incidentenbeheer tijdens een project	Elke organisatie moet: a. In de loop van de ontwikkeling van een project de procedures met betrekking tot het incidentbeheer formaliseren en valideren. Dit moet toelaten het ontwikkelde systeem te integreren in het standaard incident beheerssysteem van de organisatie. b. ervoor zorgen dat de veiligheidsconsulent op de hoogte wordt gesteld van de veiligheids- en privacy-incidenten in de loop van de ontwikkeling van een project.
5.11.11	Documentatie	Elke organisatie moet tijdens de levensloop van het project de documentatie (technisch, procedures, handleidingen, …) actueel houden.
5.11.12	Inventaris	Elke organisatie moet alle middelen inclusief aangekochte of ontwikkelde systemen toevoegen aan het beheerssysteem van de operationele middelen.
5.11.13	Audit	Elke organisatie moet voor interne en externe audit de gepaste medewerking verlenen onder de vorm van het ter beschikking stellen van personeel, documentatie, logbeheer en andere informatie die redelijkerwijze beschikbaar is.
5.11.14	Veilige project levenscyclus	Elke organisatie moet de ‘secure project lifecycle’ toepassen zoals beschreven in de bijlage C van de beleidslijn ‘Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen’.
5.11.15	Toepassingsveiligheid	Elke organisatie moet de nodige maatregelen treffen om de veiligheid te garanderen op toepassingsniveau teneinde eventuele informatie-veiligheidsinbreuken te vermijden (vertrouwelijkheid, integriteit, beschikbaarheid)[21].

5.12. Leveranciersrelaties

	Onderwerp	Minimumnorm

21 Voorbeelden van deze bedreiging zijn : SQL injection, Spoofing, Cross Site Scripting, Elevation Privilege.

	Onderwerp	Minimumnorm
5.12.1	Veilig uitbesteden aan derden	In geval van uitbesteding moet elke organisatie zich ervan vergewissen dat: a. de verplichtingen[22] inzake de verwerking van persoonsgegevens contractueel zijn vastgelegd. b. de vereisten rond informatieveiligheid en privacy overeengekomen moeten worden met derde partijen en gedocumenteerd worden om risico's te reduceren met betrekking tot toegang van derde partijen tot informatiemiddelen. c. alle relevante vereisten rond informatieveiligheid en privacy opgesteld en overeengekomen moeten worden met elk van die derde partijen die informatie van de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten aanleveren. d. overeenkomsten met derde partijen alle vereisten omvatten om risico's van informatieveiligheid en privacy te behandelen die geassocieerd zijn met ICT diensten e. de dienstverlening van derde partijen regelmatig wordt gemonitord, geëvalueerd en geauditeerd. f. wijzigingen in de dienstverlening door derden worden beheerd, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatieveiligheid en privacy. Bij het beheren dient er rekening gehouden te worden met het kritieke karakter van de betrokken systemen en processen en met her-evaluatie van risico's. g. de 'Richtlijnen rond veilig uitbesteding aan derde partijen' worden toegepast zoals beschreven in de bijlage C van de beleidslijn 'Veilig uitbesteding aan derden'.
5.12.2	Cloud computing	Elke organisatie moet ; a. wanneer ze een beroep doet op cloud-diensten conform zijn met punt 2.1 van de beleidslijn 'Cloud computing' b. wanneer ze professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud o de minimale contractuele waarborgen in acht nemen zoals ze beschreven zijn in punt 2.2 van de beleidslijn 'Cloud computing' o de informatieveiligheid voor de cloud service provider in acht nemen zoals ze beschreven zijn in punt 2.3 van de beleidslijn 'Cloud computing' o de privacy voor de cloud service provider in acht nemen zoals ze beschreven zijn in punt 2.4 van de beleidslijn 'Cloud computing'

5.13. Beheer van incidenten in verband met informatieveiligheid

	Onderwerp	Minimumnorm

22 De organisatie blijft altijd aansprakelijk voor de informatieveiligheid en de privacy van de verwerking, met inbegrip van de verwerking bij de onderaannemer(s).

	Onderwerp	Minimumnorm
5.13.1	Beheer van incidenten	Elke organisatie moet: a. procedures hebben voor het vastleggen en beheren van incidenten over informatieveiligheid of privacy en de bijhorende verantwoordelijkheden. Deze procedures moeten bekend zijn bij alle medewerkers. b. Vastleggen in de overeenkomst met de medewerkers dat elke medewerker (zowel vast of tijdelijk, intern of extern) verplicht is melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen. c. Gebeurtenissen en zwakheden over informatieveiligheid of privacy die verband houden met informatie en informatiesystemen van de organisatie zodanig kenbaar maken dat de organisatie tijdig en adequaat corrigerende maatregelen kan nemen. d. Incidenten over informatieveiligheid en privacy zo snel als mogelijk via de leidinggevende, de helpdesk, de informatieveiligheidsconsulent (CISO) of functionaris van gegevensbescherming (DPO) rapporteren. e. Bij incidenten over informatieveiligheid of privacy het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct verzamelen. f. Elk incident over informatieveiligheid of privacy formeel evalueren opdat procedures en controlemaatregelen verbeterd kunnen worden. De lessen die getrokken worden uit een incident dienen gecommuniceerd te worden naar de directie van de organisatie voor validatie en goedkeuring van verdere acties. g. de 'richtlijn rond incidentenbeheer' toepassen zoals beschreven in de bijlage C van de beleidslijn 'incidentenbeheer'

5.14. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

	Onderwerp	Minimumnorm
5.14.1	Continuïteitsbeheer	Elke organisatie moet: a. Voor alle kritieke processen en essentiële informatiesystemen een continuïteitsplan opstellen, waarin activiteiten, maatregelen en belangrijke gegevens van de processen van de organisatie worden beschreven, die tot doel hebben de onderbrekingstijd tot een aanvaardbaar niveau te beperken. b. Informatieveiligheid en privacy als een integraal onderdeel van het continuïteitsbeheer uitwerken (zie bijlage C 'Richtlijnen rond continuïteit van informatieveiligheid en privacy' van de beleidslijn 'Continuïteitsbeheer') c. een eigen continuïteitsplan hebben met minimaal aandacht aan: 1) Identificatie en documentatie van essentiële processen en bijhorende informatiesystemen van de organisatie; 2) Risico-beoordeling met invulling van kans, impact en huidige controlemaatregelen; 3) Kennis en competenties van medewerkers om essentiële processen en bijhorende informatiesystemen van de organisatie draaiende te houden of weer op te starten; 4) Wie mag wanneer en hoe wordt het continuïteitsplan geactiveerd bij een

	Onderwerp	Minimumnorm
		ernstig incident of ramp; 5) Informatie (aanvaardbaarheid van verlies van informatie); 6) Prioriteiten en volgorde van herstel; 7) Communicatie tijdens en na een ernstig incident of ramp; 8) Wie mag wanneer en hoe wordt het uitgevoerde continuïteitsplan formeel afgesloten na een ernstig incident of ramp. d. over een adequaat continuïteitsbeheer beschikken waardoor de impact van een ernstig incident of ramp en het herstel daarvan tot een aanvaardbaar niveau wordt beperkt in lijn met de verwachtingen van de organisatie. e. Het continuïteitsplan regelmatig testen en aanpassen. De resultaten van de testen moeten gecommuniceerd worden naar de directie van de organisatie voor validatie en goedkeuring van verdere acties.

5.15. Naleving

	Onderwerp	Minimumnorm
5.15.1	Naleving	Elke organisatie moet: a. periodiek een conformiteitsaudit uitvoeren met betrekking tot de situatie rond informatieveiligheid en privacy zoals beschreven in de beleidslijnen[23]. b. schending voorkomen van enige wetgeving, wettelijke, regelgevende, statutaire of contractuele verplichtingen gerelateerd aan informatieveiligheid en privacy. c. zeker stellen dat informatieveiligheid en privacy geïmplementeerd en operationeel in overeenstemming is met de verwachtingen van de directie. d. een formeel disciplinair proces hebben voor werknemers die inbreuk op de informatieveiligheid of privacy hebben gepleegd. e. 'de richtlijn rond naleving' toepassen (bijlage C van de beleidslijn 'naleving').
5.15.2	Verwerking van persoonsgebonden gegevens	Elke organisatie moet: a. regelmatig alle risico's in kaart brengen in verband met de conformiteit met de Europese verordening[24]. De geplande acties als gevolg van een hoog "residueel" risico op non-conformiteit dienen opgenomen te worden in het informatieveiligheid- en privacy-plan van de organisatie. b. In functie van de rol voor een specifieke (groep) verwerking (verwerker of verwerkings-verantwoordelijke), minimaal de volgende activiteiten uitvoeren: • de opname van de verwerking in het centraal register van de

23 Volgens gangbare goede praktijken zou een dergelijke audit minstens één keer per jaar georganiseerd moeten worden. Daarbij is het niet verboden dat de veiligheidsconsulent van een organisatie een audit uitvoert bij een andere organisatie van hetzelfde netwerk. Als de beheersinstelling van een secundair netwerk geen duidelijk zicht heeft op de informatieveiligheid- of privacy-situatie bij één van haar leden, kan zij aan het Sectoraal Comité vragen om een conformiteitsaudit uit te voeren.

24 https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_NL.pdf

	Onderwerp	Minimumnorm
		verwerkingsverantwoordelijke of van de verwerker; • een formele verantwoording voor het niet-realiseren van controlemaatregelen gericht op de naleving van de Europese verordening[25].

6. Handhaving, opvolging en herziening

Jaarlijks zal een vragenlijst opgestuurd worden naar de organisaties van het netwerk van sociale zekerheid teneinde de naleving van de minimale normen informatieveiligheid en privacy te evalueren en opmerkingen te bestuderen.

Op basis van de toegestuurde vragenlijsten, kan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid controles laten uitvoeren met betrekking tot de naleving van specifieke aspecten van de minimale normen informatieveiligheid en privacy in een organisatie.

Een wijziging van de minimale normen informatieveiligheid en privacy geeft aanleiding tot

- de voorlegging van het voorstel tot wijziging aan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid;
- de voorlegging van de gewijzigde vragenlijst aan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid;
- het opsturen van de gewijzigde en goedgekeurde minimale normen naar de verantwoordelijken voor het dagelijks bestuur van de organisaties die hun beheerscomité ervan op de hoogte brengen;
- het in werking treden van de goed goedgekeurde minimale normen het jaar volgend op het werkjaar van de goedkeuring door het Beheerscomité[26] van de Kruispuntbank van de Sociale Zekerheid (KSZ).

De onderwerpen van specifieke maatregelen die goedgekeurd werden op het niveau van het Algemeen Coördinatiecomité[27] en die nog niet opgenomen werden in een herziene versie van de minimale normen informatieveiligheid en privacy, zullen pro-actief opgenomen worden in de jaarlijkse vragenlijst.

7. Sanctie

Indien het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid vaststelt dat een organisatie tekortschiet wat de naleving van deze minimale normen informatieveiligheid en privacy betreft, kan het Comité de Kruispuntbank van de Sociale Zekerheid (KSZ) verzoeken om geen gevolg meer te verlenen aan de door die organisatie verstuurde voorleggingen. Alvorens deze maatregel kan worden genomen, zal het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid de persoon ondervragen die belast is met het dagelijks bestuur van de betrokken organisatie.

[25] pas toe of leg uit principe (“comply or explain principle”)

[26] Het Beheerscomité geeft de nodige richtlijnen inzake de toepassing van de Kruispuntbankwet en geeft adviezen over voorstellen tot wijziging van de wetten en koninklijke besluiten die op de Kruispuntbank en de werking van het netwerk van de sociale zekerheid betrekking hebben. De voogdijminister raadpleegt het Beheerscomité betreffende alle materies die hij/zij nodig acht.

[27] Het Algemeen Coördinatiecomité staat het Beheerscomité van de Kruispuntbank van de Sociale Zekerheid (KSZ) en het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid bij in de vervulling van hun opdrachten. Hiertoe is het gelast alle initiatieven voor te stellen ter bevordering en ter bestendiging van de samenwerking binnen het netwerk, en alle maatregelen voor te stellen die kunnen bijdragen tot een rechtmatige en vertrouwelijke behandeling van de sociale gegevens van persoonlijke aard.

BIJLAGE A: Toepasselijke beleidslijnen rond informatieveiligheid en privacy (versie 2017)

Hieronder staat een lijst met meer gedetailleerde beleidslijnen zoals gekozen door de werkgroep Informatieveiligheid. Voor de instellingen in het algemeen, voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO), zijn deze beleidslijnen een extra inspiratiebron waarop ze zich kunnen baseren bij de uitvoering van hun opdrachten rond informatieveiligheid en privacy. De toepassing van deze beleidslijnen behoort echter tot de verantwoordelijkheid van iedere instelling. Elke organisatie kan zelf bijkomende beleidslijnen suggereren en/of uitwerken.

Deze lijst is niet exhaustief en zal regelmatig bijgewerkt worden.

BLD RISK	**Risico-beoordeling**
BLD HR	**Personeelsgerelateerde aspecten**
BLD DATA	**Data classificatie**
BLD DESK	**Clean Desk en Clear Desk**
BLD TELE	**Telewerk**
BLD ONLINE	**Email, online communicatiemiddelen en internet gebruik**
BLD WIREL	**Draadloze netwerken**
BLD KSZ	**Gebruik van het internet om toegang te krijgen tot het netwerk van de KSZ in het kader van de verwerking van persoonsgegevens door de actoren van de sociale sector**
BLD PORTAL	**Toegangsbeheer van portalen**
BLD CRYPT	**Vercijferen**
BLD AUTH	**Authenticatiemiddel bepaling voor toepassing**
BLD DATA SEC	**Data veiligheid**
BLD PHYS	**Fysieke toegangsbeveiliging**
BLD ERASE	**Wissen van informatiedragers**
BLD LOG	**Logbeheer**
BLD MOBILE	**Mobiele toestellen**
BLD APPDEV	**Aankopen, ontwerpen, ontwikkelen en onderhouden van informatiesystemen**
BLD OUTS	**Uitbesteding aan derden**
BLD CLOUD	**Cloud**
BLD INCID	**Incidentenbeheer**
BLD BCM	**Continuïteitsbeheer**
BLD COMPLY	**Naleving**
BLD PRIV	**Verwerking van persoonsgebonden gegevens**

***** EINDE VAN DIT DOCUMENT *****