VRAGENLIJST 2018 VOOR DE EVALUATIE VAN DE MINIMALE VEILIGHEIDSNORMEN:

GECONTROLEERD JAAR 2017

Naam van de instelling (verplicht)	Benaming: ..... Adres: .... Ondernemingsnummer (KBO): 0 | | | | | | | | | |
Voornaam, Naam & email adres van de veiligheidsconsulent (CISO) (verplicht)	....
Voornaam, Naam & email adres van de adjunct veiligheidsconsulent (Adjunct CISO) (optioneel)	....
Voornaam, Naam & email adres van de functionaris voor gegevensbescherming (DPO) (optioneel)	....
Voornaam, Naam & email adres van de adjunct functionaris voor gegevensbescherming (Adjunct DPO) (optioneel)	....
Voornaam, Naam & email adres van de persoon belast met het dagelijks bestuur van de instelling (verplicht)	....

De minimale veiligheidsnormen die gepubliceerd werden op de site van de Kruispuntbank van de Sociale Zekerheid, gelden in eerste instantie 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 Zekerheid*. Door de tijd heen heeft de wetgever het toepassingsgebied van het netwerk van de Kruispuntbank uitgebreid bij toepassing van artikel 18 van voormelde wet. Naast de instellingen van sociale zekerheid maakt ook deel uit van het netwerk van de sociale zekerheid elke organisatie die van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid een machtiging verkregen heeft voor de toegang, het gebruik en het verstrekken van sociale gegevens.
Om de leesbaarheid van dit document te verhogen, dekt de term « organisatie » het hele toepassingsgebied van de minimale veiligheidsnormen zoals beschreven in de vorige paragraaf.

De organisaties moeten deze minimale veiligheidsnormen verplicht naleven 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 organisatie om de vragenlijst correct in te vullen en over de naleving van de normen te waken. Het Sectoraal Comité van de Sociale Zekerheid kan desgevallend controles ter plaatse (laten) uitvoeren teneinde op het terrein te peilen naar de naleving van de minimale veiligheidsnormen.

De vragenlijst heeft tot **doel** te evalueren en te bepalen of de veiligheidsnormen die van kracht zijn binnen de organisatie, overeenstemmen met de doelstellingen van de minimale veiligheidsnormen naargelang de specifieke situatie van de organisatie en de belangrijkheid van de te beveiligen werkingsmiddelen.

De implementatie en de verificatie van de minimale veiligheidsnormen bij derden die voor rekening van een organisatie sociale gegevens van persoonlijke aard verwerken[1], behoren in eerste instantie tot de verantwoordelijkheid van de organisatie die aan derden werkzaamheden toevertrouwt. (Art. 16 van de wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens)

De evaluatie van de antwoorden gebeurt door het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid.

1 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.

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.1	**Kernprincipes**		
5.1.1	Heeft de organisatie de kernprincipes opgenomen in haar informatieveiligheid?	☐ JA ☐ NEEN	
5.2	**Beleid voor informatieveiligheid**		
5.2.1	Beschikt de organisatie over een formeel, geactualiseerd en door de verantwoordelijke voor het dagelijks bestuur goedgekeurd beleid voor informatieveiligheid?	☐ JA ☐ NEEN	
5.2.2a	Heeft de organisatie een risicobeoordelingsproces (gebruikt bij de projecten en de processen) dat rekening houdt met de informatieveiligheid en privacy?	☐ JA ☐ NEEN	
5.2.2b	Heeft de organisatie alle risico-beoordelingen met een hoog residueel risico naar de directie gecommuniceerd?	☐ JA ☐ NEEN	
5.2.2c	Past de organisatie voor haar risico-beoordeling de principes toe zoals opgelijst in de ‘richtlijn rond risico-beoordeling’ (bijlage C van de beleidslijn ‘Risico-beoordeling’)?	☐ JA ☐ NEEN	
5.3	**Organisatie van de informatieveiligheid**		
5.3.1.1	Voert de organisatie de verplichte activiteiten uit (voor zover van toepassing) voorafgaand, tijdens, en bij de beëindiging of wijziging van dienstverband zoals beschreven in de minimale normen 5.3.1.1?	☐ JA ☐ NEEN	
5.3.1.2a	Binnen de organisatie: • is er een veiligheidsdienst onder leiding van een veiligheidsconsulent? • is er een dienst belast met de informatieveiligheid die onder de directe, functionele leiding staat van de verantwoordelijke voor het dagelijks bestuur van de organisatie? • heeft de organisatie de informatieveiligheid toegekend aan een erkende gespecialiseerde veiligheidsdienst belast met de veiligheid?	☐ JA ☐ NEEN ☐ JA ☐ NEEN ☐ JA ☐ NEEN	
5.3.1.2b	Heeft de organisatie de identiteit van haar veiligheidsconsulent en diens eventuele adjuncten meegedeeld aan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid of, wat de instellingen van het secundaire netwerk betreft, aan de verantwoordelijke instelling voor dit netwerk?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.3.1.2c	Beschikt de organisatie over een door de verantwoordelijke voor het dagelijks bestuur goedgekeurd informatieveiligheidsplan?	☐ JA ☐ NEEN	
5.3.1.2d	Beschikt de organisatie die aangesloten is op het netwerk van de Kruispuntbank over de nodige werkingskredieten die door de verantwoordelijke van de betrokken organisatie werden goedgekeurd, teneinde te kunnen voorzien in de uitvoering van haar veiligheidsplan en de uitvoering door de veiligheidsdienst van de haar opgedragen taken?	☐ JA ☐ NEEN	
5.3.1.2e	Hoeveel uren werden gepresteerd door de veiligheidsconsulent en diens adjunct(en) voor de uitvoering van de veiligheidstaken? 1) veiligheidsconsulent 2) adjunct-veiligheidsconsulent(en) Hoeveel uren opleidingen rond informatieveiligheid hebben de veiligheidsconsulent diens adjunct(en) gevolgd in het jaar? 1) veiligheidsconsulent 2) adjunct-veiligheidsconsulent(en)	 1) uren / maand 2) uren / maand 3) uren / jaar 4) uren / jaar	
5.3.1.2f	Beschikt de organisatie over procedures voor de mededeling van informatie aan de veiligheidsconsulent, zodat deze laatste over de nodige gegevens beschikt voor de uitvoering van zijn opdracht die hem toevertrouwd werd?	☐ JA ☐ NEEN	
5.3.1.3	Beschikt de organisatie over een beslissingsplatform voor de validatie en de goedkeuring van de veiligheidsmaatregelen?	☐ JA ☐ NEEN	
5.3.1.4	Wisselt de beheersorganisatie van een « secundair netwerk » minstens één keer per semester relevante informatie uit met haar secundair netwerk door een vergadering van de subwerkgroep "Informatieveiligheid" te organiseren voor de organisaties die deel uitmaken van haar netwerk. Indien ja, gelieve in de rechterkolom naast JA - NEEN - N/A de data van de vergaderingen te vermelden die georganiseerd werden tijdens het geauditeerde jaar?	☐ JA ☐ NEEN ☐ NVT	
5.3.1.5	Beschikt de organisatie die aangesloten is op het netwerk van de Kruispuntbank over procedures voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen, zodat de projectverantwoordelijke rekening kan houden met de informatieveiligheid- en privacy-vereisten?	☐ JA ☐ NEEN ☐ NVT	
	(subgroep 'Organisatie van de informatieveiligheid')		

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.3.2.1a	Neemt de organisatie de gepaste maatregelen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media (zowel mobiele opslagmedia als toestellen) enkel toegankelijk zijn voor geautoriseerde personen?	☐ JA ☐ NEEN	
5.3.2.1b	Treft de organisatie de gepaste maatregelen, in functie van het toegangsmedium, voor de informatieveiligheid van de online-toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie?	☐ JA ☐ NEEN	
5.3.2.1c	Legt de organisatie de voorwaarden op, die gedetailleerd zijn in de beleidslijn ' mobiele toestellen', bij het gebruik van privé-toestellen voor beroepsdoeleinden?	☐ JA ☐ NEEN	
5.3.2.1d	Legt de organisatie de regels op, die gedetailleerd zijn in de beleidslijn ' mobiele toestellen', bij het gebruik van de mobiele toestellen voor zowel beroepsdoeleinden als voor privé-doeleinden?	☐ JA ☐ NEEN	
5.3.2.1e	Heeft de organisatie een centraal register met de identificatie van de eigen mobiele toestellen[2] en configureert ze de nodige veiligheid voor deze toestellen (met de nodige anti-malware software en met software die alle data op het toestel vanop afstand kunnen wissen)?	☐ JA ☐ NEEN	
5.3.2.1f	Implementeert de organisatie de gepaste controles om de conformiteit van de mobiele toestellen inzake de beleidslijnen informatieveiligheid en privacy te controleren (vanop afstand via software of ter plaatse via directe controle)?	☐ JA ☐ NEEN	
5.3.2.1g	Sensibiliseert de organisatie regelmatig de gebruikers omtrent de goede praktijken inzake gebruik en hun verantwoordelijkheden (zeker in verband met het connecteren tot publieke draadloze netwerken)?	☐ JA ☐ NEEN	
5.3.2.1h	Bestaat de mogelijkheid 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?	☐ JA ☐ NEEN	
5.3.2.1i	Verbindt de organisatie zich ertoe om de privacy van de gebruiker te respecteren?	☐ JA ☐ NEEN	
5.3.2.2a	Heeft de organisatie de gepaste maatregelen getroffen, in functie van het toegangsmedium[3], voor de informatieveiligheid van de online-toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie?	☐ JA ☐ NEEN	

2 Mobiele toestellen : zie BLD Mobile voor de omschrijving

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

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.3.2.2b	Heeft de organisatie duidelijk gedragsregels en een gepaste implementatie van telewerken opgezet, gevalideerd, gecommuniceerd en onderhouden, inclusief de uitwerking van welke systemen niet, en welke systemen wel vanuit de thuiswerkplek of andere apparaten mogen worden geraadpleegd?	☐ JA ☐ NEEN	
5.3.2.2c	Heeft de organisatie de telewerk-voorzieningen van de organisatie zo ingericht dat er op de telewerk-plek (thuis, in een satellietkantoor of in een andere locatie) geen 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?	☐ JA ☐ NEEN	
5.4	**Medewerkers-gerelateerde veiligheid (Clean desk & Clear desk)**		
5.4.1	Sensibiliseert de organisatie jaarlijks iedere medewerker met betrekking tot de informatieveiligheid en privacy en voert ze jaarlijks een evaluatie uit rond de naleving van dit beleid in de praktijk (via interne enquête)?	☐ JA ☐ NEEN	
5.4.2a	Beschikt de organisatie over een beleidslijn waarbij wordt aangegeven dat de medewerking van alle medewerkers van essentieel belang is voor de informatieveiligheid en de privacy?	☐ JA ☐ NEEN	
5.4.2b	Beschikt de organisatie over een beleidslijn waarbij wordt aangegeven dat de gebruiker steeds verantwoordelijk blijft voor de informatie, ongeacht de vorm waarin deze informatie wordt opgeslagen?	☐ JA ☐ NEEN	
5.4.2c	Heeft de organisatie de toegang beveiligd door een duidelijke toegangsprocedure en heeft ze een (logisch of fysiek) toegangssysteem geïmplementeerd om elke ongeoorloofde toegang tot de organisatie te voorkomen?	☐ JA ☐ NEEN	
5.5	**Beheer van bedrijfsmiddelen**		
5.5.1a	Beschikt de organisatie over een intern classificatieschema dat in lijn is met de specifieke wetgeving terzake alsook met eventuele internationale regelgeving?	☐ JA ☐ NEEN	
5.5.1b	Beschikt de organisatie over gepaste procedures en registers voor het labelen (etiketteren) van de verwerkingen van alle in beheer zijnde informatieverzamelingen, informatiedragers en informatiesystemen in overeenstemming met het interne classificatieschema?	☐ JA ☐ NEEN	
5.5.1c	Beschikt en past de organisatie de regel toe dat de classificatie die door de soort informatie bepaald wordt ook geldt voor het hogere niveau classificatie van informatie?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.5.1d	Worden alle classificaties van alle kritieke systemen centraal vastgelegd door de eigenaren?	☐ JA ☐ NEEN	
5.5.1e	Worden alle classificaties van alle kritieke systemen jaarlijks gecontroleerd door de informatieveiligheidsconsulent (CISO) en/of de functionaris voor gegevensbescherming (DPO)?	☐ JA ☐ NEEN	
5.5.1f	Zijn de controlemaatregelen afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van de te nemen maatregelen?	☐ JA ☐ NEEN	
5.5.2	Beschikt de organisatie over een permanent bijgewerkte inventaris van het informaticamateriaal en de software?	☐ JA ☐ NEEN	
5.5.4a	Heeft de organisatie de regels verwerkt in haar beleid voor informatieveiligheid die gespecifieerd zijn in de beleidslijn 'Email, online communicatie en internet gebruik'?	☐ JA ☐ NEEN	
5.5.4b	Oefent de organisatie een permanente controle uit op het 'Email, online communicatie en internet gebruik' in het kader van de volgende doelstellingen: • bescherming van de reputatie en de belangen van de organisatie; • voorkomen van ongeoorloofde handelingen of handelingen die indruisen tegen de goede zeden of die de waardigheid van een persoon kunnen schaden; • 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; • naleving van de kernprincipes?	☐ JA ☐ NEEN	
5.5.5	Heeft de organisatie de nodige maatregelen getroffen om fysieke media, bijvoorbeeld back-ups met gevoelige gegevens, tijdens het transport te beschermen tegen niet geautoriseerde toegang?	☐ JA ☐ NEEN	
5.6	**Toegangsbeveiliging (logisch)**		
5.6.1a	Heeft de organisatie minstens één toegangsbeheerder aangesteld wanneer ze gebruik maakt van de diensten en toepassingen van het portaal van de sociale zekerheid ten behoeve van zijn gebruikers?	☐ JA ☐ NEEN	
5.6.1b	Heeft de organisatie zijn medewerkers aangezet tot het lezen en toepassen van de reglementen over het gebruik van de informatiesystemen van de portalen?	☐ JA ☐ NEEN	
5.6.1c	Wanneer de organisatie gebruik maakt van de diensten en toepassingen van het portaal van de sociale zekerheid ten behoeve van zijn gebruikers, leeft ze dan de verplichten na die gepaard gaan met het uitoefenen van de functie beheerder of medebeheerder en die beschreven zijn in de beleidslijn 'toegangsbeheer van portalen'?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.6.2	Wanneer de organisatie wil gebruik maken van het internet als toegangsmiddel tot het netwerk van de Kruispuntbank van de Sociale Zekerheid (KSZ) : • beschikt ze over een schriftelijke machtiging en afwijking van de leidende ambtenaar van de KSZ? • heeft ze strikt de voorwaarden toegepast die zijn opgesomd in de bijlage D (Voorwaarden voor toegang tot het Extranet van de Sociale Zekerheid via internet) van de beleidslijn?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
5.6.3	Heeft de organisatie de toegang tot de gegevens nodig voor de toepassing en de uitvoering van de sociale zekerheid beveiligd door middel van een identificatie-, authenticatie- en autorisatiesysteem?	☐ JA ☐ NEEN	
5.6.4	Heeft de organisatie de noodzakelijke machtigingen van het bevoegde sectoraal comité voor de toegang tot (sociale) persoonsgegevens beheerd door een andere organisatie?	☐ JA ☐ NEEN	
5.6.5	Heeft de organisatie de toegang van informatiebeheerders tot informaticasystemen beperkt door identificatie, authentificatie, en autorisatie?	☐ JA ☐ NEEN	
5.6.6	Heeft de organisatie de gepaste maatregelen getroffen opdat iedere persoon slechts toegang zou hebben tot de diensten waarvoor hij uitdrukkelijk een autorisatie heeft verkregen?	☐ JA ☐ NEEN	
5.6.7	Gebruikt de organisatie het Extranet van de sociale zekerheid voor alle externe verbindingen of de verbindingen met haar secundaire netwerk? Is voor iedere afwijking op deze maatregel een gemotiveerde aanvraag via de veiligheidsdienst van de KSZ ingediend?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
5.7	**Vercijferen**		
5.7.1	Wanneer de organisatie ‘cryptografie’ wilt toepassen : • beschikt ze over een formeel beleid voor het gebruik van cryptografische controles? • beschikt ze over een formeel beleid voor het gebruik, bescherming en levensduur van de cryptografische sleutels voor de ganse levenscyclus?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
5.8	**Fysieke beveiliging en beveiliging van de omgeving**		
5.8.1	Neemt de organisatie de nodige maatregelen om de toegang tot de gebouwen en lokalen te beperken tot de geautoriseerde personen en verricht ze een controle erop zowel tijdens als buiten de werkuren?	☐ JA ☐ NEEN	
5.8.2	Neemt de organisatie de nodige maatregelingen ter voorkoming van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.8.3a	Neemt de organisatie de nodige maatregelingen bij het gebruik van vercijfering als preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager?	☐ JA ☐ NEEN	
5.8.3b	Bij hergebruik van de informatiedrager, gebruikt de organisatie deze opnieuw in een minstens vergelijkbaar data classificatieniveau?	☐ JA ☐ NEEN	
5.8.3c	Gebruikt de organisatie een risico-beoordeling om de gepaste methode te bepalen voor het wissen van een informatiedrager?	☐ JA ☐ NEEN	
5.8.3d	Vernietigt de organisatie fysiek de informatiedrager wanneer een voor de organisatie niet aanvaardbaar residuele risico bestaat als na het wissen van de gegevens deze worden teruggevonden?	☐ JA ☐ NEEN ☐ NVT	
5.8.3e	Legt de organisatie de gepaste maatregelen voor het wissen van gegevens contractueel vast 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)?	☐ JA ☐ NEEN ☐ NVT ☐ JA ☐ NEEN ☐ NVT	
5.9	**Operationeel beheer**		
5.9.1	Heeft de organisatie zich ervan verzekerd dat er geen testen of ontwikkelingen plaatsvinden in de productieomgeving?	☐ JA ☐ NEEN	
5.9.2	Beschikt de organisatie over procedures voor het in productie stellen van nieuwe toepassingen en het aanpassen van bestaande toepassingen? Heeft de organisatie de nodige maatregelen genomen om te voorkomen dat een enkele persoon alleen de controle zou verwerven over dit proces?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
5.9.3	Beschikt de organisatie over geactualiseerde systemen ter bescherming (voorkoming, detectie en herstel) tegen malware?	☐ JA ☐ NEEN	
5.9.4	Heeft de organisatie de policy en strategie gedefinieerd om een backupsysteem te implementeren, in overeenstemming met het continuïteitsbeheer? Heeft de organisatie regelmatig de genomen backups geverifieerd?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.9.6	Kan de organisatie (die deelneemt aan het verzenden van gegevens via de Kruispuntbank) de traceerbaarheid van de identiteiten waarborgen?	☐ JA ☐ NEEN	
5.9.7	Heeft de organisatie een systeem en formele, geactualiseerde procedures geïnstalleerd die toelaten om veiligheidsinbreuken te detecteren, op te volgen en te herstellen in verhouding tot het technisch/operationeel risico?	☐ JA ☐ NEEN	
	(Subgroep 'Operationeel beheer')		

5.9.5	In verband met de logging van de toegang :
	• beschikt de organisatie over een formele procedure van logbeheer?
	• legt de organisatie de transacties, controlewerkzaamheden, activiteiten van gebruikers, uitzonderingen en informatieveiligheid- en privacy-gebeurtenissen/incidenten gestructureerd vast in afzonderlijke logbestanden?
	• wordt het logbeheer meegenomen vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om "security/privacy by design" te realiseren?
	• worden elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, gelogd in overeenstemming met de toepasselijke wetgeving en regelgeving?
	• worden de interne klokken van alle informatiesystemen van de organisatie gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron zodat een betrouwbare analyse van logbestanden op verschillende informatiesystemen altijd mogelijk is?
	• zijn de noodzakelijke tools beschikbaar of worden ze ontwikkeld om log gegevens te analyseren door de geautoriseerde personen?
	• wordt het systeemgebruik gelogd:
	  ○ automatisch?
	  ○ of door gebruik te maken van een manueel logboek?
	• worden de logbestanden beschermd tegen inzage door onbevoegden, wijzigingen en verwijderingen?
	• worden de logbestanden gedurende een overeengekomen periode bewaard, ten behoeve van toekomstig onderzoeken en controles en in overeenstemming met wetgeving en regelgeving?
	• bestaat er een georganiseerde procedure binnen de organisatie met een historiek van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd voor de raadpleging van de logbestanden?
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN
		☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
	• wordt het resultaat van logbeheer regelmatig geanalyseerd, gerapporteerd en beoordeeld ?	☐ JA ☐ NEEN	
5.10	**Communicatiebeveiliging**		
5.10.1a	Beschikt de organisatie, voor alle draadloze netwerken onder beheer van de organisatie op alle locaties, over een proces voor het up-to-date houden van een overzicht waarin de bestaande en toegestane draadloze netwerken, bijhorende veiligheidsprotocollen en alle bijhorende informatieveiligheidsmaatregelen terug te vinden zijn?	☐ JA ☐ NEEN	
5.10.1b	Leeft de organisatie, voor alle draadloze netwerken onder beheer van de organisatie op alle locaties, de richtlijnen na die beschreven zijn in bijlage C van de beleidslijn 'veilige draadloze netwerken'?	☐ JA ☐ NEEN	
5.10.2	Kijkt de organisatie na dat de netwerken gepast beheerd en gecontroleerd worden zodanig dat ze beveiligd zijn tegen bedreigingen?	☐ JA ☐ NEEN	
5.10.3	Heeft de organisatie de noodzakelijke, afdoende, gepaste en doeltreffende technische maatregelen geïmplementeerd 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?	☐ JA ☐ NEEN	
5.10.4	Heeft de organisatie een geactualiseerde cartografie van de geïmplementeerde technische[4] stromen via het Extranet van de sociale zekerheid?	☐ JA ☐ NEEN	
5.10.5	Verwerkt de organisatie elke overdracht van sociale gegevens binnen het netwerk van de sociale zekerheid zo snel mogelijk door met name elke afwijking of lacune in de elektronische overdracht te melden?	☐ JA ☐ NEEN	
5.11	**Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen**		
5.11.1	Is er bij elke project voor het verwerven, ontwikkelen en onderhouden van systemen een constructieve communicatie opgezet tussen de verschillende bij het project betrokken partijen en de veiligheidsconsulent(en)?	☐ JA ☐ NEEN	
5.11.2a	Werken alle medewerkers met de ICT middelen (die door de instelling ter beschikking worden gesteld) op basis van minimale autorisatie voor de uitvoering van hun taak?	☐ JA ☐ NEEN	

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

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.11.2b	Is er bij het ontwikkelen van de toegangsbeveiliging rekening houden met de reeds bestaande operationele systemen voor het toegangsbeheer (zoals UAM) en hun evolutie?	☐ JA ☐ NEEN	
5.11.2c	Worden de vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd? Worden deze toegangen gelogd?	☐ JA ☐ NEEN	
5.11.2e	Legt de organisatie zelf de relatie tussen het programmanummer en de identiteit van de natuurlijke persoon die het bericht verstuurt wanneer een programma ontwikkeld wordt waarin de sociale zekerheidsinstelling een programmanummer overneemt in een bericht dat ze aan de KSZ richt, en waar een natuurlijk persoon aan de basis van dit bericht ligt?	☐ JA ☐ NEEN	
5.11.2d	Heeft men het beheer van de toegangen, intern in een applicatie, zo veel mogelijk vermeden?	☐ JA ☐ NEEN	
	(Subgroep 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen')		
5.11.3	Worden bij de uitbesteding aan derden de veiligheids- en privacyvereisten contractueel vastgelegd alsook de vertrouwelijkheids- en continuïteitsclausules?	☐ JA ☐ NEEN	
5.11.4	Gebruikt de organisatie een controlelijst zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en privacy correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project?	☐ JA ☐ NEEN	
5.11.5	Voert de organisatie bij elke in productiestelling van een project een controle uit of de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden? Veiligheidsvereisten zijn ondermeer de eisen op het vlak van vertrouwelijkheid, integriteit en beschikbaarheid.	☐ JA ☐ NEEN	
5.11.6	Worden, onder de supervisie van de projectleider, de voorzieningen voor ontwikkeling, test en/of acceptatie en productie gescheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project?	☐ JA ☐ NEEN	
5.11.7b1	Wordt in de specificaties van een project opgenomen 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?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.11.7b2	Beantwoordt het logbeheer tijdens een project minimaal aan de volgende doelstellingen? • De informatie om te kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie • De identificatie van de aard van de geraadpleegde informatie • De duidelijke identificatie van de persoon	☐ JA ☐ NEEN	
5.11.7c	Heeft men rekening gehouden met reeds bestaande logbeheersystemen bij de evaluatie van logbehoeften in het kader van het project?	☐ JA ☐ NEEN	
5.11.7e	Worden de Privacy logs minimaal 10 jaar bewaard?	☐ JA ☐ NEEN	
	(subgroep 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen')		
5.11.8	Worden de deliverables (broncode, programma's, technische documenten, …) van het project geïntegreerd in het back-up beheersysteem van de organisatie zoals opgelegd in de beleidslijnen?	☐ JA ☐ NEEN	
5.11.9a	Worden, in de loop van de ontwikkeling van het project, de behoeften met betrekking tot continuïteit van de dienstverlening geformaliseerd, conform met de verwachtingen van de organisatie?	☐ JA ☐ NEEN	
5.11.9b	Worden in de softwaresystemen de herstartpunten duidelijk geïntegreerd om het hoofd te bieden aan operationele problemen? De informatie betreffende de herstartpunten maakt deel uit van het exploitatiedossier.	☐ JA ☐ NEEN	
5.11.9c	Wordt er tijdens de ontwikkeling van een project bijzondere aandacht besteed aan de back-up en herstel ("restore") van informatie?	☐ JA ☐ NEEN	
5.11.9d	Wordt er in de productieomgeving rekening gehouden met de eisen van de organisatie met betrekking tot probleemtolerantie en redundantie van de infrastructuur?	☐ JA ☐ NEEN	
5.11.9e	Wordt het continuïteitsplan en de bijhorende procedures geactualiseerd in functie van de projectevolutie, met inbegrip van continuïteitstesten?	☐ JA ☐ NEEN	
5.11.9f	Wordt er een risicoanalyse in het begin van het project uitgevoerd om de noodprocedures te definiëren?	☐ JA ☐ NEEN	
5.11.10a	Worden, in de loop van de ontwikkeling van een project, de procedures met betrekking tot het incidentbeheer geformaliseerd en gevalideerd?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.11.10b	Wordt de veiligheidsconsulent op de hoogte gesteld van de informatieveiligheids- en privacy-incidenten in de loop van de ontwikkeling van een project?	☐ JA ☐ NEEN	
5.11.11	Wordt tijdens de levensloop van het project de documentatie (technisch, procedures, handleidingen, …) actueel gehouden?	☐ JA ☐ NEEN	
5.11.12	Worden alle middelen inclusief aangekochte of ontwikkelde systemen toegevoegd aan het beheerssysteem van de operationele middelen (inventaris)?	☐ JA ☐ NEEN	
5.11.13	Wordt aan de interne en externe audit de gepaste medewerking verleend onder de vorm van het ter beschikking stellen van personeel, documentatie, logbeheer en andere informatie die redelijkerwijze beschikbaar is?	☐ JA ☐ NEEN	
5.11.14	Worden de aspecten van de 'Secure project lifecycle' toegepast . Voor meer informatie zie bijlage C van de beleidslijn 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen'?	☐ JA ☐ NEEN	
5.12	**Leveranciersrelaties**		
5.12.1a	Worden de verplichtingen inzake de verwerking van persoonsgegevens contractueel vastgelegd wanneer de organisatie werk uitbesteedt aan een leverancier?	☐ JA ☐ NEEN	
5.12.1b	Worden de vereisten rond informatieveiligheid en privacy overeengekomen met de derde partijen en gedocumenteerd om risico's te reduceren met betrekking tot toegang van derde partijen tot de informatie?	☐ JA ☐ NEEN	
5.12.1c	Hebben de leveranciers (waaraan het werk is uitbesteed en die informatie van de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten aanleveren) de vragenlijst "minimale normen leveranciers" volledig beantwoord?	☐ JA ☐ NEEN	
5.12.1d	Bevatten de overeenkomsten met derde partijen (leveranciers) alle vereisten om risico's van informatieveiligheid en privacy te behandelen geassocieerd met ICT diensten?	☐ JA ☐ NEEN	
5.12.1e	Wordt door de organisatie regelmatig de dienstverlening van derde partijen gemonitord, geëvalueerd en geauditeerd?	☐ JA ☐ NEEN	
5.12.1f	Worden de wijzigingen in de dienstverlening door derden beheerd ? Onder wijzigingen verstaan we onder andere het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatieveiligheid en privacy?	☐ JA ☐ NEEN	
5.12.1g	Worden de 'Richtlijnen rond uitbesteding aan leveranciers' toegepast zoals beschreven in de bijlage C van de beleidslijn 'Uitbesteding aan derden'?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.12.2a	Is de organisatie conform met de punten beschreven in paragraaf 2.1 van de beleidslijn 'Cloud computing' wanneer de organisatie een beroep doet op cloud-diensten?	☐ JA ☐ NEEN	
5.12.2b	Wanneer de organisatie professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud voldoet ze dan aan de minimale contractuele waarborgen en de beleidslijnen zoals ze beschreven zijn in punt 2.2, 2.3 en 2.4 van de beleidslijn 'Cloud computing'?	☐ JA ☐ NEEN	
5.13	**Beheer van incidenten in verband met informatieveiligheid**		
5.13.1a	Heeft de organisatie procedures voor het vastleggen en beheren van incidenten over informatieveiligheid of privacy met de bijhorende verantwoordelijkheden en heeft ze deze procedures bekend gemaakt aan zijn medewerkers?	☐ JA ☐ NEEN	
5.13.1b	Heeft de organisatie een 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?	☐ JA ☐ NEEN	
5.13.1c	Worden de gebeurtenissen en zwakheden over informatieveiligheid of privacy die verband houden met informatie en informatiesystemen van de organisatie zodanig kenbaar gemaakt dat de organisatie tijdig en adequaat corrigerende maatregelen kan nemen?	☐ JA ☐ NEEN	
5.13.1d	Worden de incidenten over informatieveiligheid en privacy zo snel als mogelijk via de leidinggevende, de helpdesk, de informatieveiligheidsconsulent (CISO) of functionaris van gegevensbescherming (DPO) gerapporteerd in overeenstemming met de incident procedures?	☐ JA ☐ NEEN	
5.13.1e	Worden bij incidenten over informatieveiligheid of privacy het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften (zoals onder andere de AVG regelgeving) correct verzameld?	☐ JA ☐ NEEN	
5.13.1f	Wordt elk incident over informatieveiligheid of privacy formeel gevalideerd opdat procedures en controlemaatregelen verbeterd kunnen worden en worden de lessen die getrokken worden uit een incident gecommuniceerd naar de directie van de organisatie voor validatie en goedkeuring van verdere acties?	☐ JA ☐ NEEN	
5.13.1g	Wordt de de 'richtlijn rond incidentenbeheer' toegepast zoals ze beschreven is in de bijlage C van de beleidslijn 'incidentenbeheer'?	☐ JA ☐ NEEN	
5.14	**Informatiebeveiligingsaspecten van continuïteitsbeheer**		
5.14.1a	Bestaat er een continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen van de organisatie?	☐ JA ☐ NEEN	

Norm	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
5.14.1b	Is informatieveiligheid en privacy een integraal onderdeel van het continuïteitsbeheer?	☐ JA ☐ NEEN	
5.14.1c	Heeft de organisatie een eigen continuïteitsplan ingericht met de minimale informatie zoals beschreven in de beleidslijn 'Continuïteitsbeheer'?	☐ JA ☐ NEEN	
5.14.1e	Wordt het continuïteitsplan regelmatig getest en aangepast met de nodige communicatie naar de directie voor validatie en goedkeuring?	☐ JA ☐ NEEN	
5.15	**Naleving**		
5.15.1a	Voert de organisatie periodiek een conformiteitsaudit uit met betrekking tot de situatie rond informatieveiligheid en privacy zoals beschreven in de beleidslijnen?	☐ JA ☐ NEEN	
5.15.1d	Heeft de organisatie een formeel disciplinair proces voor werknemers die inbreuk op de informatieveiligheid of privacy hebben gepleegd?	☐ JA ☐ NEEN	
5.15.1e	Wordt de 'richtlijn rond naleving' toegepast zoals ze beschreven is in de bijlage C van de beleidslijn 'naleving'?	☐ JA ☐ NEEN	
5.15.2a	Brengt de organisatie regelmatig alle risico's in kaart in verband met de conformiteit met de Europese verordening en voert ze de nodige acties uit als gevolg van een hoog "residueel" risico op non-conformiteit?	☐ JA ☐ NEEN	
5.15.2b	Heeft de organisatie de nodige en up-to-date centrale registers van de verwerkingsverantwoordelijke of van de verwerker en heeft ze een formele verantwoording voor het niet-realiseren van controlemaatregelen gericht op de naleving van de Europese verordening voor de specifieke (groep) verwerking?	☐ JA ☐ NEEN	

Gelieve de ingevulde vragenlijst uiterlijk vóór **20 mei 2018** terug te sturen naar de dienst Informatieveiligheid en Interne Audit van de Kruispuntbank van de Sociale Zekerheid.

Voorwaarde die nageleefd moet worden door de instellingen van het secundaire netwerk:

De instellingen van het secundaire netwerk sturen de ingevulde vragenlijst terug naar de voogdijinstelling die de ontvangen lijsten overmaakt aan de dienst Informatieveiligheid en Interne Audit van de Kruispuntbank vóór de hierboven vermelde datum.

Datum en handtekening van de veiligheidsconsulent (CISO) of van de functionaris voor gegevensbescherming (DPO) (optioneel)	..... Datum Handtekening
Datum en handtekening van de persoon belast met het dagelijks bestuur van de instelling **(verplicht)**	..... Datum Handtekening

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